United States General Accounting Office

GAO

Report to Congressional Requesters

July 2003

INFORMATION TECHNOLOGY

Executive Office for U.S. Attorneys Needs to Institutionalize Key IT Management Disciplines

GAO-03-751

July 2003

INFORMATION TECHNOLOGY

Executive Office for U.S. Attorneys Needs to Institutionalize Key IT Management Disciplines

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-751, a report to congressional requesters

Why GAO Did This Study

The Executive Office for United States Attorneys (EOUSA) of the Department of Justice is responsible for managing information technology (IT) resources for the United States Attorneys' Offices. GAO was asked to determine the extent to which EOUSA has institutionalized key IT management capabilities that are critical to achieving Justice's strategic goal of improving the integrity, security, and efficiency of its IT systems.

What GAO Recommends

To strengthen EOUSA's IT management capacity and to increase its chances of effectively leveraging IT to improve its mission performance, GAO recommends that the Attorney General direct the Director of EOUSA to (1) designate institutionalization of each of the IT management disciplines as priorities and (2) develop and implement action plans in each of the four IT disciplines to address the weaknesses that are identified in this report. EOUSA agreed with the majority of GAO's findings and recommendations, and stated that it will address most of the recommendations. It also stated that it has made notable progress in institutionalizing the IT management disciplines, particularly information security, and that each is currently an office priority.

www.gao.gov/cgi-bin/getrpt?GAO-03-751.

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

To varying degrees, EOUSA has partially defined and implemented certain IT management disciplines that are critical to successfully achieving the Justice Department's strategic goal of improving the integrity, security, and efficiency of its IT systems. However, it has yet to institutionalize any of these disciplines, meaning that it has not defined existing policies and procedures in accordance with relevant guidance, and it has yet to fully implement what it has defined. In particular, while EOUSA has developed an enterprise architecture—a blueprint for guiding operational and technological change—the architecture was not developed in accordance with certain best practices. In addition, while the office has implemented certain process controls for selecting, controlling, and evaluating its IT investments, it has not yet implemented others that are necessary in order to develop an effective foundation for investment management. Further, it has not implemented important management practices that are associated with an effective security program. In contrast, it has defined—and is implementing on a major system that we reviewed—most, but not all, of the management practices associated with effective systems acquisition.

Institutionalization of these IT management disciplines has not been an agency priority and is not being guided by plans of action or sufficient resources. Until each discipline is given the priority it deserves, EOUSA will not have the IT management capabilities it needs to effectively achieve the department's strategic goal of improving the integrity, security, and efficiency of its IT systems.

EOUSA's Institutionalization of Four Key IT Management Disciplines

Management discipline	Fully Institutionalized?	Comment
Enterprise architecture management	No	Has an approved enterprise architecture but, for example, has yet to develop a policy for maintaining it.
IT investment management	No	Has several basic elements of proper IT investment management but has not yet, for example, used its defined investment selection process.
Information security management	No	Is not fully satisfying any of the tenets of effective security, such as monitoring the effectiveness of security controls and promoting security awareness.
System acquisition management	No	Is successfully employing most of the practices associated with effective software acquisition management on one key project but does not have, for example, a policy for software acquisition planning.

Source: GAO.

Contents

Letter 1

Results in Brief 2
Background 3
EOUSA Has Yet to Institutionalize Key IT Management Disciplines 6
Conclusions 23
Recommendations 23
Agency Comments and Our Evaluation 25

Appendixes

Appendix I: Objective, Scope, and Methodology 29
Appendix II: Assessment of ECMS Acquisition Practices against Level 2 of SEI's Software Acquisition Capability Maturity Model 32
Appendix III: Comments from the Department of Justice 44
GAO Comments 50
Appendix IV: GAO Contact and Staff Acknowledgments 54
GAO Contact 54
Acknowledgments 54

Tables

Table 1: Summary of Version 1.0 of GAO's EA Management Maturity Framework Stages 9
Table 2: Assessment of EOUSA's EA Efforts against GAO's EA Maturity Framework 10
Table 3: The Five Stages of GAO's ITIM Maturity Framework 12
Table 4: Assessment of EOUSA's ITIM Efforts against Stage 2 of GAO's ITIM Maturity Framework 13
Table 5: SA-CMM Levels and Descriptions 21
Table 6: Assessment of ECMS Acquisition against SEI's SA-CMM Level 2 Key Process Area 22
Table 7: Software Acquisition Planning 32
Table 8: Solicitation 34
Table 9: Requirements Development and Management 36
Table 10: Project Management 38
Table 11: Contract Tracking and Oversight 40
Table 12: Evaluation 42

Figures

Figure 1: Simplified Diagram of EOUSA's Network Connections 4
Figure 2: Estimated IT Expenditures for Fiscal Year 2003 6

Abbreviations

CIO	chief information officer
EA	enterprise architecture
ECMS	Enterprise Case Management System
EOUSA	Executive Office for United States Attorneys
GWAC	Governmentwide Acquisition Contracts
IRB	Investment Review Board
IT	information technology
ITIM	IT investment management
JCN	Justice Consolidated Network
LIONS	Legal Information Office Network System
SA-CMM	Software Acquisition Capability Maturity Model
SEI	Software Engineering Institute
USAO	United States Attorneys' Office
VANITS	Value Added Niche Information Technology Service
VPN	virtual private network
WAN	wide-area network

G A O
Accountability * Integrity * Reliability

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

July 25, 2003

The Honorable F. James Sensenbrenner, Jr.
Chairman
The Honorable John Conyers, Jr.
Ranking Minority Member
Committee on the Judiciary
House of Representatives

The Honorable Christopher Cannon
Chairman
The Honorable Melvin L. Watt
Ranking Minority Member
Subcommittee on Commercial and Administrative Law
House of Representatives

This report is one of a series in response to your request that we evaluate the management activities of the Executive Office for United States Attorneys (EOUSA) and the U.S. Attorneys' Offices (USAO). As part of this request, you asked us to determine the extent to which EOUSA—the organization responsible for managing information technology (IT) resources for the USAOs—has institutionalized key IT management capabilities critical to achieving the Department of Justice's strategic goal of improving the integrity, security, and efficiency of its IT systems. As agreed, to meet this objective, we focused on whether EOUSA had institutionalized four important IT management disciplines: enterprise architecture management, investment management, system acquisition management, and security management. Research shows that these disciplines are institutionally employed by leading public and private sector organizations. They are also provided for in legislation and federal guidance.[1]

Details on our objective, scope, and methodology are in appendix I.

[1]See, for example, Clinger-Cohen Act of 1996, Public Law 104-106; Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (February 1996); Office of Management and Budget, *Funding Information Systems Investments*, Memorandum M-97-02; and National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST SP 800-14 (September 1996).

Results in Brief

To varying degrees, EOUSA has partially defined and implemented each of four key IT management disciplines that are critical to successfully achieving the Department of Justice's strategic goal of improving the integrity, security, and efficiency of its IT systems. However, it has yet to institutionalize any of these disciplines—meaning that it has not defined its policies and procedures in accordance with relevant guidance—and it has yet to fully implement what it has defined. In particular, while EOUSA has an enterprise architecture—a blueprint for guiding operational and technological change—it has not developed the architecture in accordance with certain best practices. In addition, while the office has implemented certain process controls for selecting, controlling, and evaluating its IT investments, it has not yet implemented others that are necessary in order to develop an effective foundation for investment management. Further, it has not implemented important management practices that are associated with an effective security program, such as implementing and monitoring security policies and controls and promoting security awareness. To its credit, the office has defined—and is implementing on a major system—most, though not all, of the management practices associated with effective systems acquisition.

The institutionalization of these IT management disciplines has not been a sufficiently high priority for EOUSA, as evidenced by the absence of plans for fully implementing best practices for each discipline and, in some cases, an absence of requisite resources. Until each discipline is given the priority it deserves, EOUSA will not have the IT management capabilities that are critical to effectively achieving the Justice Department's strategic goal of improving the integrity, security, and efficiency of its IT systems. We are making recommendations to the Attorney General to strengthen management of each of these disciplines.

In its written comments on a draft of this report, EOUSA agreed with our specific findings for three of the four IT management disciplines, and stated that it would address the weaknesses that we identified in each. However, it stated that its security program is strong, citing a number of security initiatives, including ones recently planned or started that are consistent with our recommendations for addressing security weaknesses. We do not question the initiatives that EOUSA cited. However, our analysis of its security program, including these initiatives, identified serious security weaknesses, and as a result, we do not agree that EOUSA's security program is strong. Further, it stated that institutionalization of each of the IT disciplines is currently an office priority and that the state of its IT

management capabilities is not an impairment to achieving departmental strategic goals. However, it did not dispute either of our two reasons for concluding otherwise; namely, that it did not have a plan for fully implementing best practices for each discipline, and it had not allocated adequate resources to support such a plan. EOUSA's comments are summarized and evaluated in the Agency Comments and Our Evaluation section of this report.

Background

U.S. Attorneys prosecute criminal cases brought forward by the federal government, prosecute and defend civil cases in which the United States is a party, and collect debts owed to the federal government that are administratively uncollectible. EOUSA was established in 1953 as a component of the Department of Justice to, among other things, provide general executive assistance and administrative and operational support to the 93 USAOs located throughout the 50 states, the District of Columbia, Guam, the Marianas Islands, Puerto Rico, and the U. S. Virgin Islands[2] and to coordinate with other Department of Justice organizational units and other federal agencies on behalf of the U.S. Attorneys. One of EOUSA's key responsibilities is managing the USAOs' IT resources, including preparing their annual IT budget submissions and supporting their acquisition and maintenance of IT assets.

IT plays an important role in helping the USAOs meet their mission objectives and, according to EOUSA planning documents, the USAOs' reliance on IT is to increase in response to expected growth in the number and complexity of their cases. Currently, EOUSA manages an IT environment consisting of central and distributed computing and communication resources in Washington, D.C., and 93 USAOs, respectively. Connectivity among these offices, Justice headquarters, and Justice's Data Center in Rockville, MD,[3] is through a virtual private network (VPN)[4] connection on the Justice Consolidated Network (JCN), with such security

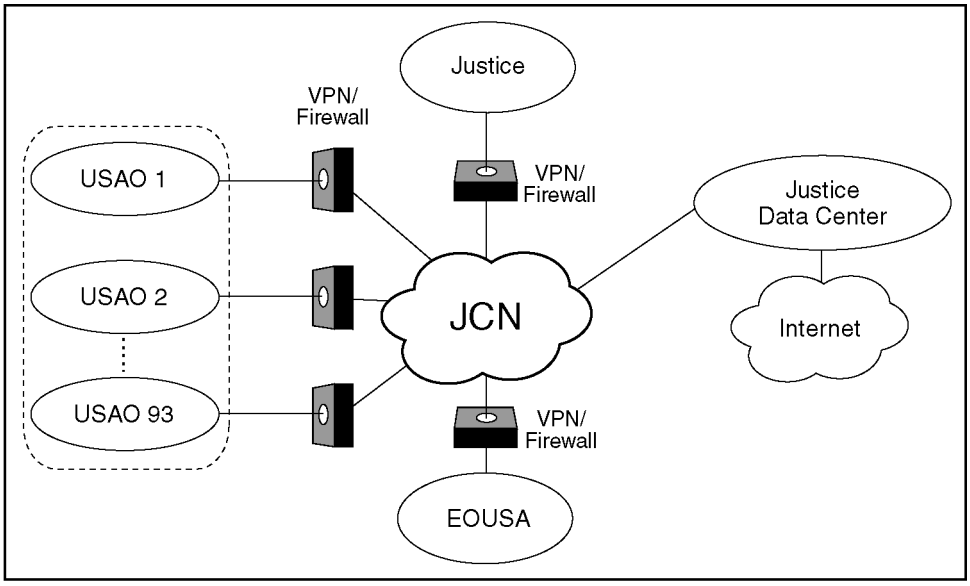
[2]U.S. Attorneys' Offices and their branches comprise over 240 sites.

[3]Access to the Internet and to research services is provided through Justice's Rockville, MD, Data Center.

[4]A virtual private network uses a public or shared telecommunication infrastructure to provide remote users with secure access to an organization's network.

safeguards as firewalls[5] between USAO local area networks and JCN. The VPN/firewall combination, which provides the foundation for secure communications between EOUSA and the sites mentioned above, is currently being replaced. Figure 1 generally depicts EOUSA's network topology. The USAOs' support is also provided by such application systems as the Legal Information Office Network System, which is a case management system that compiles, maintains, and tracks information about defendants, crimes, criminal charges, court events, and witnesses, and the Victim Notification System, which notifies crime victims of the status of their cases and assists with checking compliance with regulations and policies concerning victim notification.

Figure 1: Simplified Diagram of EOUSA's Network Connections



Sources: U.S. Department of Justice, Executive Office for U.S. Attorneys, Strategic Plan for Information Management: Technology for the EOUSA and United States Attorneys' Offices FY 2002 - 2006 (Version 2, May 2002).

[5]Network firewalls are devices or systems that control the flow of traffic between networks with different security requirements. Organizations employ firewalls to prevent unauthorized access to their respective systems and resources.

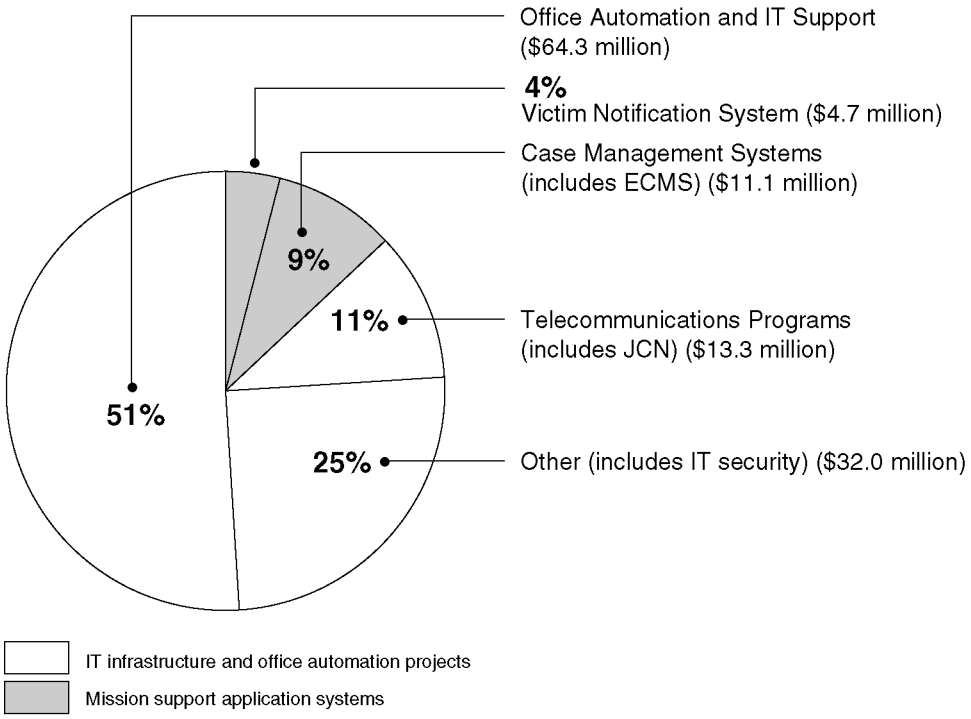
Recognizing the importance of IT to achieving the USAOs' mission, EOUSA appointed a Chief Information Officer (CIO) in May 2001 and assigned the CIO accountability and responsibility for managing central and distributed IT resources and services, including

- managing the IT budget for the office and all of the USAOs;
- developing and acquiring new systems, including case management systems, and providing support for existing systems;
- managing network, telephone, and video communications; and
- securing IT assets (data, applications, and supporting networks).

In fiscal year 2003, EOUSA reports that it plans to spend approximately $125 million on about 20 initiatives. Roughly $110 million of this amount is to be spent on IT infrastructure and office automation projects (e.g., telecommunications programs). The remainder is to be spent on acquiring mission support systems (e.g., Enterprise Case Management System (ECMS),[6] Victim Notification System) and maintaining existing ones. Figure 2 shows the breakdown of estimated expenditures for fiscal year 2003.

[6]ECMS is intended to replace the Legal Information Office Network System (LIONS) and a system for reporting data stored in LIONS and to be the enterprise solution for managing and tracking case workload within the USAOs.

Figure 2: Estimated IT Expenditures for Fiscal Year 2003



Source: GAO analysis of EOUSA data.

EOUSA Has Yet to Institutionalize Key IT Management Disciplines

Research into the IT management practices that are employed by leading public- and private-sector organizations has identified key institutional IT management disciplines that are interrelated and critical to ensuring, among other things, the integrity, security, and efficiency of IT systems. These disciplines are also addressed in legislation and federal guidance.[7]

[7]See, for example, Clinger-Cohen Act of 1996, Public Law 104-106; Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (February 1996); Office of Management and Budget, *Funding Information Systems Investments*, Memorandum M-97-02; and National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST SP 800-14 (September 1996).

They include

1. *enterprise architecture management*, which involves defining, maintaining, and implementing an institutional blueprint that defines both the business and the supporting technology of the organization's current and target operating environments and a roadmap to achieve the target environment;

2. *IT investment management*, which involves selecting, controlling, and evaluating a portfolio of investments within the context of an enterprise architecture;

3. *IT security management*, which involves protecting the integrity, confidentiality, and availability of an organization's IT assets (e.g., data, application systems, and networks) and reducing the risks of tampering, unauthorized intrusions and disclosures, and disruption of operations.

4. *system acquisition management*, which involves managing selected investments (system projects) in a manner that increases the probability of promised system capabilities being delivered on time and within budget.

As we have previously reported,[8] to successfully institutionalize these disciplines, organizations should develop integrated plans to guide their efforts that (1) specify measurable goals, objectives, and milestones; (2) specify needed resources; and (3) assign clear responsibility and accountability for accomplishing well-defined tasks. In addition, these plans should be approved by senior management. In implementing these plans, it is important that organizations allocate adequate resources and measure and report progress against planned commitments and that appropriate corrective actions be taken to address deviations.

EOUSA has defined and implemented each of the four IT management disciplines mentioned above to some degree. However, none has been institutionalized, meaning that they are not fully defined in accordance

[8]U.S. General Accounting Office, *Information Technology:* INS Needs to Better Manage the Development of Its Enterprise Architecture, GAO/AIMD-00-212 (Washington, D.C.: August 2000); *Information Technology: DLA Needs to Strengthen Its Investment Management Capability*, GAO-02-314 (Washington, D.C.: March 2002).

with best practices and what has been defined has not been fully implemented. While these disciplines have been given attention since the recent appointment of the CIO, they have not been treated as priorities, in that action plans needed for successful institutionalization have not been developed or resourced. As a result, EOUSA is currently limited in its ability to meet Justice's strategic goal of improving its IT systems, and the USAOs will be challenged in their ability to effectively and efficiently meet their mission goals and priorities.

EOUSA Is Not Performing Important Practices Associated with Effective Enterprise Architecture Management

An enterprise architecture (EA) is an investment blueprint that defines, both in logical terms (including business functions and applications, work locations, information needs and users, and the interrelationships among these variables) and in technical terms (including hardware, software, data communications, and security) how an organization operates today ("as is"), how it intends to operate tomorrow ("to be"), and a roadmap for transitioning from today to tomorrow. The development, maintenance, and implementation of architectures are recognized hallmarks of successful public and private organizations. According to a guide published by the federal CIO Council,[9] effective architecture management consists of a number of core elements.

In February 2002, we published version 1.0 of our EA management maturity framework, which arranges the core elements of the CIO Council's guide into five hierarchical stages.[10] The framework provides an explicit benchmark for gauging the effectiveness of architecture management and provides a roadmap for making improvements. Table 1 summarizes the framework's five stages of maturity.

[9]Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001).

[10]U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: February 2002). We issued version 1.1 of the framework in April 2003—*A Framework for Assessing and Improving Enterprise Architecture Management*, GAO-03-584G—but did not use it for our evaluation because we had already completed our audit work evaluating EOUSA against the initial framework.

Table 1: Summary of Version 1.0 of GAO's EA Management Maturity Framework Stages

Stage	Description
Stage 5: Leveraging the EA to manage change (includes all elements in stage 4)	This stage entails, among other things, incorporating the EA into corporate decision making to (1) avoid unwarranted overlap across investments, (2) enable maximum systems interoperability, and (3) ensure selection and funding of IT investments with manageable risks and returns.
Stage 4: Completing the EA products (includes all elements in stage 3)	This stage is characterized by having EA products that have been approved by the EA steering committee (established in stage 2) or an investment review board, and by the CIO.
Stage 3: Developing the EA products (includes all elements in stage 2)	This stage focuses on developing EA products according to the selected framework, methodology, tool, and established management plans.
Stage 2: Building the EA management foundation	This stage focuses on assigning EA management roles and responsibilities, establishing plans for developing EA products, and committing the resources necessary for developing these products.
Stage 1: Creating EA awareness	This stage is characterized either by no plans to develop and use an EA or by plans that do not demonstrate an awareness of the value of having and using an EA.

Source: GAO.

EOUSA has satisfied many of the framework's core elements. Specifically, it has satisfied about 80 percent of the elements associated with building the EA management foundation—stage 2 of our EA management maturity framework—and half of the 12 core elements associated with higher maturity stages. At stage 2, it has established a chief architect and has selected a framework (the Federal Enterprise Architecture Framework) and, according to officials, selected a tool (the Enterprise Architecture Management System) to serve as a repository for its EA artifacts. At the higher stages of our framework, the CIO, for example, approved a version of an EA in May 2002 that describes the "as is" and "to be" environments for its core business functions.

However, the office has yet to satisfy several of the core elements that are critical to effective EA management. For example, a committee or group representing the enterprise has not yet been established to guide and oversee the development of future versions of the architecture. Instead, the current version of its architecture has been primarily guided and directed by the CIO's office. Until a committee or group representing the enterprise

is established, there is increased risk that the architecture will not represent a corporate decision-making tool and will not be viewed and endorsed officewide as such a tool.

Another example is the absence of a written or approved policy for maintaining the EA. Without a documented, approved policy for EA maintenance that, for example, assigns responsibility and accountability for configuration management and version control, EOUSA risks allowing its architecture to become outdated and irrelevant, thus limiting its effectiveness in selecting and guiding IT investments.

EOUSA does not have a written plan of action for strengthening EA management and evolving the current version of its EA, because, according to the CIO, developing such a plan is not a priority. Table 2 shows EOUSA's performance in addressing the core elements of our maturity framework.

Table 2: Assessment of EOUSA's EA Efforts against GAO's EA Maturity Framework

Stage	Core element	Satisfied?	Comments
Stage 5: Leveraging the EA for managing change (includes all elements from stage 4)	Written/approved policy exists for EA maintenance.	No	According to agency officials, there is no written/ approved policy for EA maintenance.
	EA steering committee, investment review board, or agency head has approved EA.	No	The EA has not been reviewed by any steering committee or investment review board or by the agency head.
	Metrics exist for measuring EA benefits.	No	According to agency officials, metrics for measuring EA benefits have not been developed.
Stage 4: Completing architecture products (includes all elements from stage 3)	Written/approved policy exists for IT investment compliance with EA.	No	While there are criteria for ranking IT investments that call for determining compliance with the EA, no written/approved policy addresses this.
	EA products describe the enterprise's business—and the data, applications, *and* technology that support it.	Yes	EA products describe EOUSA's core business functions and the data, applications, and technology that support them.
	EA products describe the "as is" environment, the "to be" environment, and a sequencing plan.	Yes	EA products describe the "as is" environment, the "to be" environment, and a sequencing plan.
	Agency CIO has approved EA.	Yes	The CIO approved the EA in May 2002.

(Continued From Previous Page)

Stage	Core element	Satisfied?	Comments
Stage 3: Developing architecture products (includes all elements from stage 2)	Written/approved policy exists for EA development.	No	According to agency officials, there is no approved policy for EA development.
	EA products are under configuration management.	No	Although agency officials reported that EA products are under configuration management, they could not provide documentation to support this statement.
	EA products describe *or will describe* the enterprise's business—and the data, applications, *and* technology that support it.	Yes	EA products describe core business functions and the data, applications, and technology that support them.
	EA products describe or *will describe* the "as is" environment, the "to be" environment, *and* a sequencing plan.	Yes	EA products describe the "as is" environment, the "to be" environment, and a sequencing plan.
	EA scope is enterprise-focused.	Yes	EA products describe the "as is" and "to be" environments for the enterprise's core business functions.
Stage 2: Building the EA management foundation	Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	No	There is no committee or group representing the enterprise that is responsible for directing, overseeing, or approving the EA. The CIO is currently responsible for direction, oversight, and approval of the architecture.
	Program office responsible for EA development exists.	Yes	Roles and responsibilities for developing the EA were assigned to a group of individuals.
	Chief architect exists.	Yes	The CIO has been designated as the chief architect.
	EA is being developed using a framework and an automated tool.	Yes	The EA was developed using the Federal Enterprise Architecture Framework. In addition, agency officials reported that they are using the Enterprise Architecture Management System as their EA tool.
	EA plans call for describing the enterprise in terms of business, data, applications, or technology.	Yes	EA products describe core business functions and the data, applications, and technology that support them.
	EA plans call for describing "as is" environment, "to be" environment, or sequencing plan.	Yes	EA products describe the "as is" environment, the "to be" environment, and a sequencing plan.
Stage 1: EA awareness	Agency is aware of EA.	Yes	In August 2002, the CIO issued a memo to agency staff notifying them of the need to use the EA to inform investment management decisions.

Source: GAO.

EOUSA Has Not Established Key Capabilities Needed to Effectively Manage IT Investments

Effective IT investment management provides for evaluating each proposed and ongoing investment, based on EA alignment and measurable risks and returns and for selecting and controlling these investments as a portfolio of competing investment options. We have developed a framework that defines and measures an organization's maturity in IT investment management (ITIM) and provides a basis for improving investment management.[11] This framework, which is based on the IT investment management practices of leading private- and public-sector organizations, is structured to permit progression through five maturity stages (shown in table 3). Each maturity stage consists of critical processes and key practices that should be implemented for an organization to become more effective in managing its IT investments.

Table 3: The Five Stages of GAO's ITIM Maturity Framework

Stage	Description
Stage 5: Leveraging IT for strategic outcomes	Investment benchmarking and IT-enabled change management techniques are deployed to strategically shape business outcomes.
Stage 4: Improving the investment process	Process evaluation techniques focus on improving the performance and management of the organization's IT investment portfolio.
Stage 3: Developing a complete investment portfolio	Comprehensive techniques are in place for selection and control of the IT investment portfolio that incorporate benefit and risk criteria linked to mission goals and strategies.
Stage 2: Building the investment foundation	Repeatable investment control techniques are in place and the key foundation capabilities have been implemented.
Stage 1: Creating investment awareness	IT management processes are ad hoc, project-centric, and have widely variable outcomes.

Source: GAO.

According to the framework, the first key step toward an effective investment management process is to build the investment foundation. An

[11]U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft), GAO/AIMD-10.1.23 (Washington, D.C.: May 2000).

organization with this foundation (stage 2 maturity) has attained repeatable, successful investment control processes and basic selection processes at the project level. Successful management at this level allows an organization to measure the progress of existing IT projects and to identify variances in cost, schedule, and performance expectations by following established, disciplined processes. The organization should also be able to take corrective action, if appropriate, and should possess basic capabilities for selecting new project proposals. To accomplish this level of basic control, an organization should establish an investment board, identify the business needs and opportunities to be addressed by each project, and use this knowledge in the selection of new proposals.

The office has satisfied two of the critical processes for stage 2, but it has not satisfied the other three. Specifically, it has established an investment governing board, known as the Investment Review Board (IRB) and developed a guide to direct its operations. It is also defining project needs in alignment with the agency's mission goals. However, the office has not, for example, defined procedures for project oversight. In addition, while an IT project and systems inventory exists as part of its "as is" architecture, a policy specifying how it will be used for investment management purposes has not been defined. Until EOUSA satisfies all critical processes for stage 2, it will not have the foundation it needs to build its investment management capability and it will not have an effective investment process. Table 4 summarizes our assessment of stage 2 capabilities.

Table 4: Assessment of EOUSA's ITIM Efforts against Stage 2 of GAO's ITIM Maturity Framework

Critical process	Description	Satisfied?	Comments
IT investment board operation	Define and establish (1) the governing board(s) responsible for selecting, controlling, and evaluating IT investments and (2) a guide directing the board(s) operations.	Yes	A governing board (the IRB) has been defined and established, and guidance directing the board's operations exists.
IT project oversight	Regularly oversee each IT project's progress toward cost and schedule milestones, using established criteria, and require corrective actions when milestones are not achieved.	No	According to agency officials, projects are managed using earned value management [a] to regularly determine project progress and control project costs and schedules. However, there are no procedures defining how the investment board is to regularly oversee each project's progress and require corrective actions when milestones are not achieved.

(Continued From Previous Page)

Critical process	Description	Satisfied?	Comments
IT project and system identification	Create and maintain an IT project and systems inventory to assist in managerial decision making.	No	An IT project and systems inventory exists as part of the EA. However, there is no policy defining how this inventory is to be used in managerial decision making.
Business needs identification for IT projects	Ensure that each IT project supports the organization's business needs and meets users' needs.	Yes	Business needs and associated users have been identified, and users participate in the management of the project. We verified this for the Enterprise Case Management System project, which officials told us is representative of how they intend to acquire systems.
Proposal selection	Ensure that an established, structured process is used to select new IT proposals.	No	A selection process using risk and return criteria is defined. However, officials stated that this selection process has not yet been used.

Source: GAO.

[a]Earned value is a management technique that relates resource planning to schedules and to technical cost and schedule requirements. There are two major objectives of an earned value system: to encourage contractors to use effective internal cost and schedule management control systems, and to permit the customer to rely on timely data produced by those systems for determining product-oriented contract status.

EOUSA has not demonstrated that maturing its IT investment management process is a priority by developing a plan for doing so and devoting resources to execute the plan. Until the office develops and implements a plan for establishing mature IT investment management processes (including all critical processes for building the investment management foundation), EOUSA will not have the full suite of capabilities it needs to ensure that project selection and control processes are repeatable or that it has the best mix of investments to meet agency priorities.

EOUSA Has Not Implemented Effective Security Practices

Effective information security management is critical to EOUSA's ability to ensure the reliability, availability, and confidentiality of its information assets, and thus it is fundamental to its ability to perform its mission. Our research into public- and private-sector organizations with strong information security programs shows that leading organizations' programs include (1) establishing a central security focal point with appropriate resources, (2) continuously assessing business risks, (3) implementing and maintaining policies and controls, (4) promoting awareness, and (5) monitoring and evaluating the effectiveness of policies and controls.[12]

Currently, EOUSA is not fully satisfying any of these tenets of effective security. In addition, it has not demonstrated that institutionalizing effective security practices is a priority by developing a plan to guide its efforts to address security weaknesses and committing resources to perform essential security functions. Until such a plan is developed and effectively implemented, data, systems, and networks are at risk of inadvertent or deliberate misuse, fraud, improper disclosure, or destruction—possibly without detection. For example, the reliability and integrity of case information may be compromised, or sensitive crime victim information may be improperly disclosed.

Central Security Focal Point Is Established but Has Not Been Appropriately Resourced

According to our framework, central management of key security functions is the foundation of an effective information security program, because it allows knowledge and expertise to be incorporated and applied on an enterprisewide basis. Having a central security focal point supported by appropriate resources is especially important for managing the increased risks associated with a highly connected computing environment, such as JCN, where security weaknesses in one segment of an organization's network can compromise the security of another segment's IT assets. In addition, centralizing the security management function provides a focal point for coordinating the activities associated with the other four elements of a strong information security program.

[12]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

In June 2001, EOUSA appointed a security officer with responsibility for centrally managing all aspects of IT security. However, EOUSA has not assigned sufficient staff to adequately carry out these responsibilities. For example, no staff has been assigned to monitor firewall logs[13] or support the development of a centrally managed IT security training program—activities that fall under the security officer's purview. Each of these activities is discussed further in the following sections.

Officials said that they recognize the need for additional staff resources to perform these activities. They also stated that they were in the process of hiring two people to support security functions, but they agreed that this would still not allow for performance of key security responsibilities. Without an appropriately resourced security program, security breaches may not be detected or addressed in a timely manner, awareness of security requirements across the organization may be inconsistent, and vulnerabilities in the current IT environment may not be appropriately addressed.

Risks Have Not Always Been Assessed

According to our framework, identifying and assessing business risks is an essential step in determining what IT security controls are needed and what resources should be invested in these controls. Federal guidance advocates performing risk assessments at least once every 3 years—or when a significant change in a system or the systems environment (e.g., new threats) has occurred. These assessments should address the risks that are introduced through connections to other networks and the impact on an organization's mission should network security be compromised. In line with this guidance, EOUSA's certification and accreditation[14] process requires that a risk assessment be completed for each system before any office can use it.

[13]Logs keep track of accesses to and attempts to access the networks that the firewalls are intended to secure.

[14]Certification is the technical and nontechnical evaluation that is conducted to verify that IT systems comply with security requirements. Accreditation is the formal declaration that the appropriate safeguards have been properly implemented and that the residual risk is acceptable.

According to EOUSA, a major system that recently underwent EOUSA's certification and accreditation process is the replacement for the existing firewall/VPN system. This system is intended to be the foundation for secure communications between EOUSA, Justice, and the geographically dispersed USAOs. Accordingly, we analyzed this system and found that while the firewall/VPN replacement system has been certified and accredited, the existing firewall/VPN system—which was deployed in 1996 and, as of May 9, 2003, was operating at 75 of the 240 sites[15]—had not had a risk assessment performed and had not been certified and accredited. Officials told us that they have not performed such an assessment on this network because (1) it is not cost-effective to use limited resources to perform an assessment on a network that is to be fully replaced by June 30, 2003, and (2) the risks inherent in the network are minimal, given that it resides on Justice's JCN, for which they said they assume Justice had performed risk assessments.

We agree that it does not make sense at this point to perform a risk assessment on the existing firewall/VPN system given that the replacement system is expected to be fully deployed by the end of June 2003. However, this does not change the fact that EOUSA has operated the network for about 7 years without understanding its exposure to risk. This is particularly important, because EOUSA officials could not provide us with evidence to support the assumption that Justice had performed a risk assessment for JCN. Moreover, previous studies have shown that Justice has had long-standing weaknesses in several aspects of its IT security program.[16] According to EOUSA, its recently established certification and accreditation program will not allow this to happen again.

Key Security Controls Have Not Been Implemented

According to our framework, risk-based, cost-effective security policies and related technology controls (such as firewalls configured to explicit rules and intrusion detection devices[17] located to monitor key network assets) and procedural controls (such as contingency plans) are needed to

[15]EOUSA is responsible for IT operations at 93 geographically dispersed USAOs and their branches, which comprise about 240 sites.

[16]U.S. Department of Justice, *FY 2000 Performance Report-FY 2002 Performance Plan, April 2001*; U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Justice*, GAO-03-105 (January 2003).

[17]Intrusion detection devices are software or hardware systems that monitor network traffic and help identify cyberthreats.

protect a system from compromise, subversion, and tampering. Federal and Justice guidance also advocate establishing these policies and controls.

While EOUSA is guided by many Justice security policies, it has not yet implemented key security controls that are needed to satisfy them. For example, CIO officials told us that the existing firewall/VPN system, which, as of May 9, 2003, was operating at 75 sites, is not based on explicit firewall rules. Moreover, according to these officials, no intrusion detection devices monitor the wide-area network (WAN)[18] routers, firewalls, and VPN devices. Rather, the intrusion detection devices that are currently implemented are located only within the local area network environment (i.e., within a USAO). Also, the contingency plan developed for the replacement firewall/VPN system was not prepared according to federal guidelines. For example, the contingency plan does not specify procedures for notifying recovery personnel or assessing damage to systems. CIO officials told us that they had not implemented these security controls because, as previously noted, they believe the risks inherent in the network are minimal given that it resides on Justice's JCN, for which they said they assumed Justice had performed risk assessments. However, as previously stated, EOUSA provided no evidence to support this assumption, and Justice has had longstanding security weaknesses.

Until EOUSA implements security controls, it may be unaware of vulnerabilities, increasing the risk that intruders may take control of network devices or that data passing through its firewalls can be read or manipulated. In addition, EOUSA may not be able to respond to security breaches adequately and in a timely manner. This is particularly threatening given the sensitivity of the information used by the USAOs in performing their work.

EOUSA Does Not Adequately Promote User Awareness

According to our framework, promoting user awareness through education and training is essential to successfully implementing information security policies, achieving user understanding of security policies, and ensuring that security controls are instituted properly. This is because computer users—and others with access to information resources—are not able to comply with policies of which they are unaware or which they do not fully understand. Our framework suggests that a central group be tasked with

[18]A wide-area network is a network that provides data communications to a large number of independent users and spans a relatively large geographical area.

educating users about current information security risks and helping to ensure consistent understanding and administration of policies.

As previously mentioned, the security officer is responsible for promoting awareness of computer security. However, the security officer does not carry out this responsibility because provision of the resources to do so has not been viewed as an agency priority. According to the security officer, each district is thus responsible for managing its own IT training program, and the security officer does not know to what extent these programs address awareness of computer security. Without a centralized approach to security education and training, the security officer cannot adequately ensure that users are consistently aware of or fully understand the organizational policies and procedures with which they are expected to comply, thus risking the integrity, reliability, and confidentiality of data and systems. According to EOUSA officials, they plan to hire staff to develop and implement a centralized program by August 2003.

EOUSA Is Not Monitoring the Effectiveness of Security Controls

Our framework recognizes the need to continuously monitor controls, through tests and evaluations, to ensure that the controls have been appropriately implemented and are operating as intended. Further, Justice's policy requires annual testing of security controls and requires EOUSA to (1) verify that the policies and procedures in component organizations are consistent with this policy and (2) enforce compliance with component and Justice security policies, including identifying sanctions and penalties for noncompliance. In addition, our framework and related best practices—as well as Justice's own policy—advocate keeping summary records of security incidents, to allow measurement of the frequency of various types of violations and the damage suffered from these incidents. This type of oversight is critical because it enables management to identify problems and their causes—and to make the necessary corrections.

CIO officials told us that testing has never been conducted to determine whether EOUSA's policies and procedures are consistent with Justice's and whether security controls are generally effective. According to these officials, testing has not been a priority because they assumed that Justice was performing tests of the WAN environment. However, Justice officials told us that, although they had evaluated the contractor's management of the WAN's circuits, they had not performed any tests to determine the effectiveness of technical and other controls associated with the WAN. The lack of testing heightens the risk that individuals both within and outside Justice could compromise EOUSA's external and internal security controls

to gain extensive unauthorized access to its networks and to networks to which it is connected.

EOUSA officials also told us that, contrary to Justice's policy, they do not maintain summary records of security incidents. Specifically, the production firewall/VPN software and routers at over 240 locations do not have audit logs that are activated, and the replacement routers, firewalls, and VPN devices are being implemented with no audit logs activated. According to these officials, they have not activated the audit logs because resources have not been allocated to provide for this security control. This lack of auditing heightens the risk of undetected intruders using EOUSA's systems to modify, bypass, or negate its firewalls and routers. Additionally, without these audit logs the office would be unable to reconstruct security-related incidents.

EOUSA Is Employing Important Acquisition Management Practices on a Key System

Rigorous and disciplined system acquisition processes and practices can reduce the risk of fielding systems that do not perform as intended, are delivered late, or cost more than planned. The Software Engineering Institute (SEI), recognized for its expertise in acquiring software-intensive systems, has published models and guides for determining an organization's acquisition process maturity. One of those models, referred to as the Software Acquisition Capability Maturity Model (SA-CMM),[19] addresses an organization's acquisition management ability.[20] The SA-CMM model defines organizational maturity according to five levels (see table 5).

[19]Carnegie Mellon University's Software Engineering Institute, *Software Acquisition Capability Maturity Model, Version 1.02*, CMU/SEI-99-TR-002 (April 1999).

[20]EOUSA officials told us that they primarily acquire their systems.

Table 5: SA-CMM Levels and Descriptions

Level	Description
Level 5: Optimizing	Continuous process improvement is empowered by quantitative feedback from the process and from piloting innovative ideas and technologies.
Level 4: Quantitative	Detailed measures of the acquisition processes, products, and services are quantitatively and qualitatively understood and controlled.
Level 3: Defined	The acquisition organization's software acquisition process is documented and standardized. All projects use an approved, tailored version of the organization's standard process for acquiring their products and services.
Level 2: Repeatable	Basic management processes for acquisition projects are established to plan all aspects of the acquisition, manage requirements, track project team and contractor team performance, manage the project's cost and schedule baselines, evaluate the products and services, and successfully transition to its support organization. The necessary process discipline is in place to repeat earlier successes on projects in similar domains.
Level 1: Initial	The acquisition process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined and success depends on individual effort.

Source: SEI.

According to SEI, level 2 (the repeatable level) demonstrates that basic management processes, known as key process areas, have been established to track performance, cost, and schedule, and that the organization has the means to repeat earlier successes on similar projects. An organization that has these processes in place is in a much better position to successfully acquire software-intensive systems than an organization that does not.

As a Justice component, EOUSA must comply with all departmental policies and procedures, including Justice's system development life-cycle management guidance. Since EOUSA officials told us that the Enterprise Case Management System (ECMS), which is intended to be the enterprise solution for managing and tracking case workload within the USAOs, is the first acquisition effort to follow Justice guidance from its inception, we compared this project, and the Justice guidance used to manage it, against SEI's SA-CMM, and we found that the project was being managed in accordance with the majority of the applicable level 2 practices. Table 6 represents a summary of our findings for this acquisition (see app. I for an expanded analysis).

Table 6: Assessment of ECMS Acquisition against SEI's SA-CMM Level 2 Key Process Area

SA-CMM level 2 key process area	Description	Total key practices	Key practices performed	Key practices not performed
Software acquisition planning	Ensure that reasonable planning for the acquisition is conducted and that all elements of the project are included.	**15**	13	2
Solicitation	Ensure that award is made to the contractor most capable of satisfying the specified requirements.	**18**	16	2
Requirements development and management	Establish a common and unambiguous definition of acquisition requirements to be used by the acquisition team, the system's users, and the contractor.	**14**	14	0
Project management	Manage the activities of the project office and supporting contractor(s) to ensure a timely, efficient, and effective acquisition.	**16**	16	0
Contract tracking and oversight	Ensure that the activities under contract are being performed in accordance with contractual requirements and that products and services will satisfy contract requirements.	**17**	16	1
Evaluation	Determine that the acquired products and services satisfy contract requirements before accepting and supporting them.	**15**	6	9

Source: GAO.

More specifically, the office has performed all of the key practices in the *requirements development and management* and *project management* key process areas. These include (1) establishing a written policy for developing and managing system-related contractual requirements; (2) having bi-directional traceability between the contractual requirements and the contractor's work products and services; (3) measuring and reporting to management on the status of requirements development and management activities; (4) designating responsibility for project management; (5) keeping plans current during the life of the project as re-planning occurs, issues are resolved, requirements are changed, and new risks are discovered; and (6) tracking the risks associated with cost, schedule, resources, and the technical aspects of the project.

EOUSA has also performed the majority of the key practices in the remaining four process areas. However, it does not have written policies for either the *contract tracking and oversight* or the *software acquisition planning* key process areas. Policies in general are key to establishing well-defined and enduring processes and procedures. In these two areas, policies would ensure that the office's approach to tracking and overseeing contractors and planning the acquisition is defined in a repeatable and

measurable fashion. In addition, during the *solicitation* process, the office did not document its plans for solicitation activities, which would provide those involved with objectives for the solicitation process and a defined way to manage and control solicitation activities and decisions. In *evaluation*, the office has yet to satisfy 9 of the 15 required practices. Officials told us that they intend to satisfy them but that they do not have a plan for addressing those practices or for implementing all of the required practices on future system acquisitions. According to these officials, developing such a plan is currently not a priority.

By developing and implementing a plan for satisfying all of these key process areas on ECMS and future acquisitions, EOUSA can increase its chances of successfully acquiring needed system capabilities on time and within budget.

Conclusions

EOUSA has taken important steps to define and implement four key IT management disciplines. Nevertheless, key aspects of each discipline have yet to be institutionalized, leaving the office challenged in its ability to achieve the department's strategic goal of improving the integrity, security, and efficiency of its IT systems. Critical to the office's success going forward will be treating institutionalization of each of these management disciplines as priority matters by developing integrated plans of action for addressing the weaknesses that we identified in each and effectively implementing these plans—including assignment of appropriate resources and measurement and reporting of progress. Without taking these steps, EOUSA is unlikely to fully establish the IT management capabilities it needs.

Recommendations

To strengthen the office's IT management capacity and increase its chances of improving the integrity, security, and efficiency of its IT systems, we recommend that the Attorney General direct the EOUSA Director to treat institutionalization of EA management, IT investment management, IT security management, and system acquisition management as priorities by developing and implementing action plans to address the weaknesses in each discipline that are identified in this report. These plans should, at a minimum, provide for accomplishing the following:

For *EA management*,

- establish a committee or group representing the enterprise that is responsible for directing, overseeing, or approving the EA;
- ensure that EA products are under configuration management;
- define, approve, and implement a policy for IT investment compliance with the EA;
- specify metrics for measuring EA benefits; and
- define, approve, and implement a policy for maintaining the EA.

For *IT investment management*,

- regularly oversee each IT project's progress toward cost and schedule milestones, using established criteria, and require corrective actions when milestones have not been achieved;
- define and implement a policy for using the IT project and systems inventory for managerial decision making; and
- ensure that an established, structured process is used to select new IT proposals.

For *IT security management*,

- allocate the appropriate resources to enable the responsibilities of the security officer to be fully performed;
- ensure that risk assessments are performed on all existing and future systems;
- implement intrusion detection devices to monitor activity at the routers, firewalls, and VPN devices, and implement other network security controls as noted in the report;
- develop and implement a centralized approach to security education and training; and

- perform regular tests to determine compliance with policies and procedures and the effectiveness of security controls.

For *system acquisition management*,

- develop and implement a policy for contract tracking and oversight;
- develop and implement a policy for system acquisition planning; and
- address the remaining key practices associated with *evaluation* as ECMS progresses in the life cycle; and
- ensure that the Software Engineering Institute acquisition practices identified in this report are used in future system acquisitions.

In developing these plans, the Director should ensure that each plan (1) is integrated with the other three plans; (2) defines clear and measurable goals, objectives, and milestones; (3) specifies resource needs; and (4) assigns clear responsibility and accountability for implementing the plan. In implementing each plan, the Director should ensure that the needed resources are provided and that progress is measured and reported periodically to the Attorney General.

Agency Comments and Our Evaluation

In written comments on a draft of this report signed by the EOUSA Director (reprinted in app. III), the office agreed with our findings relative to enterprise architecture management, IT investment management, and system acquisition management. EOUSA also agreed with our recommendations in these three areas and stated that it intends to implement the recommendations. However, EOUSA stated that it disagreed with our findings and our recommendations regarding information security management, although at the same time it cited certain actions that it intends to take, such as implementing a centralized security training program and monitoring security audit logs, that are consistent with our security findings and associated recommendations. Further, the office disagreed that the state of its efforts to institutionalize best management practices in the four areas is due to it not treating each area as an office priority. It also disagreed with our conclusion that the state of its efforts to institutionalize best practices currently limits its ability to meet Justice's strategic goal of improving its IT systems, and that the USAOs will be challenged in their ability to effectively and efficiently meet mission goals

and priorities. Each of these three areas of disagreement is addressed below.

First, with respect to information security management, EOUSA stated that it has one of the strongest security programs in Justice, and perhaps the federal government. To support this statement, the office cited 10 security initiatives it has implemented, such as certification and accreditation of more than eight systems, real-time encryption of all data in laptops and handheld devices, and conduct of vulnerability assessments and penetration testing. It also noted, among other things, that it had added 10 field security positions and 2 headquarters positions, and that its data are monitored 24 hours a day, seven days a week, and have never been compromised. We do not question these statements concerning the office's information security program and associated activities because (1) the purpose and scope of our review was not to compare EOUSA to other Justice component organizations or other federal agencies, and thus EOUSA's relative standing is not relevant to the findings in our report and (2) the message of our report is not that EOUSA has not taken steps to improve its information security posture, but rather that the office's information security management efforts, including ongoing and complete improvement steps, are weak in a number of areas relative to information security management best practices. Accordingly, we make recommendations aimed at addressing identified weaknesses, including a recommendation to implement network intrusion detection devices and other security controls. While EOUSA's comments cited plans that are consistent with many of our security-related recommendations, it disagreed with the recommendation relative to its wide area network on the grounds that this network is managed, secured, and monitored by Justice and Sprint. We understand that the WAN is not managed by EOUSA, and accordingly our recommendation was aimed at actively monitoring the network routers, firewalls, and VPN devices, which are managed by EOUSA. To avoid any confusion about this recommendation, we have clarified its wording to better reflect our intentions. Similarly, in light of the recent progress that EOUSA has made replacing its VPN system, we have adjusted our finding and recommendation concerning the office's exposure to risk from its old VPN system.

Second, with respect to our statements that EOUSA has not treated institutionalization of each of the four IT management disciplines—enterprise architecture management, IT investment management, system acquisition management, and information security management—as agency priorities, the office stated that these statements were unfair and

that it did not agree with them. To support its position, EOUSA made the following two points: (1) it has made tremendous progress, as evidenced by our report recognizing those best practices that it is satisfying, and (2) it has received the highest level of support from Justice, as evidenced by the establishment of the EOUSA CIO position in 2001, the progress that has been made in the last 2 years compared to other Justice component organizations, and EOUSA's being viewed by Justice senior management as a leader in IT management. We do not challenge EOUSA's two points because they are not relevant to our position regarding treating institutionalization of each of the four IT management disciplines as agency priorities. Our position is based on two facts that EOUSA did not dispute: (1) plans for addressing the weaknesses cited in our report do not exist and (2) limitations in resources to address these weaknesses were cited by EOUSA officials as the reason why the weaknesses exist. In our view, if each of these areas were an agency priority, then plans would be in place to address the weaknesses, and resources to execute the plans would be committed.

Third, with respect to our conclusion that EOUSA is currently limited in its ability to meet Justice's strategic goal of improving its IT systems, and that the USAOs are thereby challenged in their ability to effectively and efficiently meet their mission goals and objectives, the office disagreed but did not offer any comments to counter our conclusion beyond those cited above. Given that any organization's ability to effectively leverage technology is determined in large part by its institutionalized capabilities in these four IT disciplines, we have not modified our conclusion.

EOUSA provided additional comments that have been incorporated in the report as appropriate. EOUSA's written comments are reproduced in appendix III, along with our detailed evaluation of each comment.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will send copies of this report to interested congressional committees. We will also send copies to the Director of the Office of Management and Budget, the Attorney General of the United States, the EOUSA Director, and the EOUSA CIO. We will also

send copies to others upon request. In addition, copies will be available at no charge on our Web site at www.gao.gov.

Should you or your offices have questions on matters discussed in this report, please contact me at (202) 512-3439. I can also be reached by E-mail at hiter@gao.gov. An additional GAO contact and staff acknowledgments are listed in appendix IV.

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

Objective, Scope, and Methodology

Our objective was to determine the extent to which the Executive Office for United States Attorneys (EOUSA) has institutionalized key information technology (IT) management capabilities to achieve the Department of Justice's strategic goal of improving the integrity, security, and efficiency of its IT systems. To meet this objective, we focused on whether EOUSA had institutionalized four key IT management disciplines: enterprise architecture management, IT investment management, information security management, and system acquisition management.

- To evaluate EOUSA's enterprise architecture (EA) management, we first solicited responses to an EA management questionnaire, reviewed EA plans and products, and interviewed officials to verify their responses. Next, we compared the information that we had collected with GAO's February 2002 EA management maturity framework[1] to determine the extent to which EOUSA was employing effective EA management practices. This framework is based on the *Practical Guide to Federal Enterprise Architecture*, published by the Chief Information Officers' (CIO) Council.[2] We did not use the revised framework issued in April 2003[3] because, by then, we had already completed our work.

- To evaluate EOUSA's IT investment management (ITIM), we used GAO's ITIM framework[4] and assessed the extent to which EOUSA had satisfied the *critical processes* associated with stage 2 of the five-stage framework—building the investment foundation. We focused on stage 2 processes because officials told us that they had only recently begun defining and implementing the specific practices that are associated with this stage. To conduct our assessment, we reviewed relevant EOUSA and Justice policies, procedures, guidance, and documentation—including the office's investment management guide and associated memorandums, project proposals, and budget

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

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

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

[4]U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Exposure Draft), GAO/AIMD-10.1.23 (Washington, D.C.: May 2000).

documents. We also interviewed the CIO and the senior official who is responsible for implementing IT investment management. We then compared this information with our maturity framework to determine the extent to which the office was employing effective IT investment management practices.

- To evaluate EOUSA's information security management, we used our executive guide for information security management,[5] as well as Justice policy and guidance and relevant EOUSA *U.S. Attorney Procedures*.[6] We reviewed internal Justice and other reports identifying security weaknesses at Justice and EOUSA and information on how these weaknesses will be addressed. We also reviewed the certification and accreditation package and the deployment schedule for the virtual private network[7] that the office is currently deploying, because EOUSA and the USAOs rely on this network to carry out its mission. We interviewed Justice officials and EOUSA officials within the Office of the CIO about the office's security management.

- To evaluate EOUSA's system acquisition management, we used the Software Engineering Institute's Software Acquisition Capability Maturity Model,[8] focusing on six of the seven key process areas that are defined for level 2 of the model's five-level maturity scale.[9] We focused on level 2 processes because they represent the minimum level of maturity needed to effectively manage system acquisition projects. We used the office's acquisition of the Enterprise Case Management System as a case study because officials stated that it is representative of how

[5]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[6]See, for example, U.S. Department of Justice, *Information Technology Security* (DOJ 2640.2D (July 2001) and *EOUSA*, *Access to Sensitive But Unclassified IT Resources*, USAP 3-16.010.30.001(M) (March 2002).

[7]A virtual private network uses a public or shared telecommunication infrastructure to provide remote users with secure access to an organization's network.

[8]Carnegie Mellon University's Software Engineering Institute, *Software Acquisition Capability Maturity Model*, *Version 1.02*, CMU/SEI-99-TR-002 (April 1999).

[9]The six key process areas that we evaluated are *software acquisition planning*, *solicitation*, *requirements development and management*, *project management*, *contract tracking and oversight*, and *evaluation*. We did not include the seventh key process area—*transition to support*—in our evaluation because the system that we assessed had not yet progressed to the point that this process area was relevant.

they intend to acquire systems. In addition, this system will be critical in providing fundamental support to the U.S. Attorneys as they work to achieve mission goals. We reviewed key project documentation, such as the concept of operations, project plan, and requirements traceability matrix, and we interviewed system acquisition officials. We also reviewed the Justice guidance used to manage the project. We then compared this information to the Software Acquisition Capability Maturity Model to determine the extent to which the office was employing effective system acquisition management practices.

We performed our work at EOUSA headquarters in Washington, D.C., from November 2002 to May 2003, in accordance with generally accepted government auditing standards.

Assessment of ECMS Acquisition Practices against Level 2 of SEI's Software Acquisition Capability Maturity Model

Table 7: Software Acquisition Planning

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for planning the software acquisition.	No	EOUSA does not have a written policy for planning the software acquisition.
Commitment 2	Responsibility for software acquisition activities is designated.	Yes	Responsibility for software acquisition activities was designated to the ECMS project manager.
Ability 1	A group that is responsible for planning the software acquisition exists.	Yes	A group responsible for planning exists and includes the project manager, administrative contract officer's technical representative, and assistant directors of Case Management staff.
Ability 2	The acquisition organization provides experienced software acquisition management personnel to support project software acquisition planning.	Yes	The acquisition organization provided experienced software acquisition management personnel to support project software acquisition planning.
Ability 3	Adequate resources are provided for software acquisition planning activities.	Yes	According to EOUSA officials, adequate resources were provided for software acquisition planning activities.
Activity 1	Software acquisition planning personnel are involved in system acquisition planning.	Yes	Software acquisition planning personnel were involved in system acquisition planning.
Activity 2	The project's software acquisition planning is accomplished in conjunction with system acquisition planning.	Yes	The project's software acquisition planning was accomplished in conjunction with system acquisition planning.
Activity 3	The software acquisition strategy for the project is developed and documented.	No	There is no software acquisition strategy document.
Activity 4	Software acquisition planning addresses the elements of the software acquisition process.	Yes	Software acquisition planning addresses most critical elements of the software acquisition process.
Activity 5	The project's software acquisition planning is documented, and the planning documentation is maintained over the life of the project.	Yes	Software acquisition planning information is included in the project management plan, which has been updated once.
Activity 6	Life-cycle support of the software is included in software acquisition planning documentation.	Yes	Certain life-cycle support provisions (user training, system growth) are documented in the project management plan.
Activity 7	Life-cycle cost and schedule estimates for the software products and services being acquired are prepared and independently reviewed.	Yes	Life-cycle cost and schedule estimates for the initial release of ECMS were prepared by the project team and independently reviewed by the administrative contract officer's technical representative.
Measurement 1	Measurements (e.g., planned vs. completed works) are made and used to determine the status of the software acquisition planning activities and resultant products.	Yes	Measurements (e.g., estimated vs. actual cost and schedule) were made by the project team and used to determine the status of the software acquisition planning activities and resultant products.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Verification 1	Software acquisition planning activities are reviewed by acquisition organization management on a periodic basis.	Yes	The project team reviews software acquisition planning activities on a periodic basis.
Verification 2	Software acquisition planning activities are reviewed by the project manager on both a periodic and event-driven basis.	Yes	The project manager reviews software acquisition planning activities on both a periodic and event-driven basis.

Source: Key practice data from SEI; analysis and comments from GAO.

Table 8: Solicitation

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for the conduct of the solicitation.	Yes	The acquisition organization used the Department of Transportation's Value Added Niche Information Technology Services (VANITS) vehicle, which provides federal, state, and local government clients with access to specialized technology services and support.
Commitment 2	Responsibility for the software portion of the solicitation was designated.	Yes	Responsibility for the software portion of the solicitation was designated to a technical point of contact and an administrative contract officer's technical representative.
Commitment 3	A selection official was designated to be responsible for the selection process and the decision.	Yes	The technical point of contact and the administrative contract officer's technical representative were responsible for the selection process and the decision.
Ability 1	A group that is responsible for coordinating and conducting the solicitation activities exists.	Yes	A group consisting of assistant directors of the information technology staff exists. With the technical point of contact as the chair, this group conducted an evaluation of vendors' proposals.
Ability 2	Adequate resources were provided for the solicitation activities.	Yes	Adequate resources were provided for solicitation activities. EOUSA budgeted and paid a fee for using services provided under the VANITS vehicle.
Ability 3	Individuals performing the solicitation activities have experience or receive training.	Yes	According to EOUSA officials, individuals performing the solicitation activities have formal training or experience.
Ability 4	The groups supporting the solicitation (e.g., end user, system engineering, and application domain experts) receive orientation on the solicitation's objectives and procedures.	No	The supporting groups received an orientation, but this did not cover solicitation procedures.
Activity 1	The project's solicitation activities were performed in accordance with its plans.	No	The project team did not document its plans for solicitation activities.
Activity 2	Solicitation activities are conducted in a manner compliant with relevant laws, policies, and guidance.	Yes	The project team followed standard procedures required by the Governmentwide Acquisition Contracts (GWAC).
Activity 3	The software and evaluation requirements are incorporated into the solicitation package and resulting contract.	Yes	The project team incorporated the software and evaluation requirements into the solicitation package and resulting contract.
Activity 4	The project's proposal evaluation activities were performed in accordance with its plans.	Yes	According to EOUSA officials, the project's proposal evaluation activities were performed in accordance with its plans.
Activity 5	Cost and schedule estimates for the software activity were prepared.	Yes	Cost and schedule estimates for the software activity were prepared by the project team.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Activity 6	The software cost and schedule estimates were independently reviewed for comprehensiveness and realism.	Yes	Software cost and schedule estimates were independently reviewed for comprehensiveness and realism by the administrative contracting officer's representative.
Activity 7	The selection official uses proposal evaluation results to support his or her decision to select an offerer.	Yes	The selection official used proposal evaluation results to support his decision.
Activity 8	The project team and the offerer(s) review the project's software requirements and plans during negotiations to ensure mutual understanding.	Yes	The team reviewed four proposals and asked contractors to provide presentations to ensure mutual understanding.
Measurement 1	Measurements were made and used to determine the status of the solicitation activities and resultant products.	Yes	The VANITS program office kept the project team informed of the status of all activities. Measurements used to determine the status included the length of time taken for each activity.
Verification 1	The activities for solicitation were reviewed by acquisition organization management on a periodic basis.	Yes	The activities for solicitation were reviewed bi-weekly by the designated selection official or acquisition organization management.
Verification 2	The activities for solicitation were reviewed by the project manager or designated selection official on both a periodic and an event-driven basis.	Yes	The activities for solicitation were reviewed by the project manager on both a periodic and an event-driven basis.

Source: Key practice data from SEI; analysis and comments from GAO.

Table 9: Requirements Development and Management

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for developing and managing software-related requirements.	Yes	The project management plan includes guidelines for defining and controlling technical and nontechnical (software-related) requirements.
Commitment 2	Responsibility for requirements development and management is designated.	Yes	The ECMS project team is responsible for requirements development and management.
Ability 1	A group that is responsible for performing requirements development and management activities exists.	Yes	A Joint Application Development group is responsible for performing requirements development. The contractor is responsible for performing requirements management.
Ability 2	Adequate resources are provided for requirements development and management activities.	Yes	According to EOUSA officials, adequate resources were provided for requirements development and management activities.
Ability 3	Individuals performing requirements development and management activities have experience or receive training.	Yes	According to EOUSA officials, individuals performing requirements development and management activities have experience or received training.
Activity 1	The project team performs its activities in accordance with its documented requirements development and management plans.	Yes	EOUSA officials reported that the project team performs its activities in accordance with its documented requirements development and management plans.
Activity 2	The project team develops, baselines, and maintains software-related contractual requirements.	Yes	According to EOUSA officials, the project team develops, baselines, and maintains software-related contractual requirements.
Activity 3	The project team appraises requests for changes to system requirements for their impact on the software being acquired.	Yes	The project team reviews requests for changes to system requirements for their impact on ECMS.
Activity 4	The project team appraises all changes to the software-related contractual requirements for their impact on performance, architecture, supportability, system resource utilization, and contract schedule and cost.	Yes	The project team reviews all changes to the software-related contractual requirements for their impact on performance, architecture, supportability, system resource utilization, and contract schedule and cost.
Activity 5	Bi-directional traceability between the contractual requirements and the contractor team's software work products and services is maintained throughout the effort.	Yes	Bi-directional traceability between the contractual requirements and the contractor's team software work products and services is maintained by the project team.
Activity 6	The end user and other affected groups are involved in the development of all software-related contractual requirements and any subsequent change activity.	Yes	EOUSA officials reported that the end user and other affected groups are involved in the development of all software-related contractual requirements and any subsequent change activity.
Measurement 1	Measurements are made and used to determine the status of the requirements development and management activities and resultant products.	Yes	Measurements are made and used by the project team to determine the status of the requirements development and management activities and resultant products.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Verification 1	Requirements development and management activities are reviewed by acquisition organization management (and the contractor) on a periodic basis.	Yes	Requirements development and management activities are reviewed by the project team (and the contractor) on a periodic basis.
Verification 2	Requirements development and management activities are reviewed by the project manager on both a periodic and event-driven basis.	Yes	Requirements development and management activities are reviewed by the project manager on both a periodic and event-driven basis.

Source: Key practice data from SEI; analysis and comments from GAO.

Table 10: Project Management

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for executing the software project.	Yes	A policy memo was issued requiring all information technology projects to follow a streamlined life-cycle methodology.
Commitment 2	Responsibility for project management is designated.	Yes	Responsibility for project management is designated to the ECMS project manager.
Ability 1	A team that is responsible for performing the project's software acquisition management exists.	Yes	A team that is responsible for performing the project's software acquisition management exists. It includes a project manager and case management staff.
Ability 2	Adequate resources for the project team are provided for the duration of the software acquisition project.	Yes	According to EOUSA officials, adequate resources for the project team are provided for the duration of the software acquisition project.
Ability 3	When project trade-offs are necessary, the project manager is permitted to alter the performance, cost, or schedule software acquisition baseline.	Yes	When project trade-offs are necessary, the project manager is permitted to alter the performance, cost, or schedule software acquisition baseline after appropriate review.
Ability 4	The project team has experience or receives training in project software acquisition management activities.	Yes	EOUSA officials reported that the project team members have experience or received training in project software acquisition management activities.
Activity 1	The project team performs its activities in accordance with its documented software acquisition management plans.	Yes	EOUSA officials reported that the project team performs its activities in accordance with its project management plan.
Activity 2	The roles, responsibilities, and authority for the project functions are documented, maintained, and communicated to affected groups.	Yes	The roles, responsibilities, and authority for the project functions are documented in the ECMS project plan, maintained, and communicated to affected groups.
Activity 3	The project team's commitments, and changes to commitments, are communicated to affected groups.	Yes	The project team's commitments, and changes to commitments, are communicated to affected groups via an on-line discussion forum.
Activity 4	The project team tracks the risks associated with cost, schedule, resources, and the technical aspects of the project.	Yes	Project-wide risks are documented in the risk management plan. Ancillary risks that affect project execution, and plans for mitigating those risks, are documented in the weekly reports.
Activity 5	The project team tracks project issues, status, execution, funding, and expenditures against project plans and takes action.	Yes	According to EOUSA officials, the project team tracks project issues, status, execution, funding, and expenditures against project plans and takes action.
Activity 6	The project team implements a corrective action system for the identification, recording, tracking, and correction of problems discovered during the software acquisition.	Yes	The project team identifies, records, and tracks issues using Rational's ClearQuest product. These data are then used to correct problems discovered during the software acquisition. The team is moving toward using Merant's PVCS Dimensions software.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Activity 7	The project team keeps its plans current during the life of the project as re-planning occurs, issues are resolved, requirements are changed, and new risks are discovered.	Yes	The project team updates its plans during the life of the project as re-planning occurs, issues are resolved, requirements are changed, and new risks are discovered.
Measurement 1	Measurements are made and used to determine the status of project management activities and the resultant products.	Yes	Measurements are made and used by the ECMS project team to determine the status of project management activities and the resultant products.
Verification 1	Project management activities are reviewed by acquisition organization management on a periodic basis.	Yes	Project management activities are reviewed by acquisition organization management on a bi-weekly basis.
Verification 2	Project management activities are reviewed by the project manager on both a periodic and an event-driven basis.	Yes	Project management activities are reviewed by the project manager on both a periodic and an event-driven basis.

Source: Key practice data from SEI; analysis and comments from GAO.

Table 11: Contract Tracking and Oversight

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for the contract tracking and oversight of the contracted software effort.	No	The acquisition organization does not have a written policy for the contract tracking and oversight of the contracted software effort.
Commitment 2	Responsibility for contract tracking and oversight is designated.	Yes	Responsibility is designated to the project manager and the administrative contracting officer's representative.
Commitment 3	The project team includes contracting specialists in the execution of the contract.	Yes	These specialists include the operations staff, the contract officer's technical representative, and contracting and procurement staff.
Ability 1	A group that is responsible for managing contract tracking and oversight activities exists.	Yes	The project management team is responsible for managing contract tracking and oversight activities.
Ability 2	Adequate resources are provided for contract tracking and oversight activities.	Yes	According to EOUSA officials, adequate resources are provided for contract tracking and oversight activities.
Ability 3	Individuals performing contract tracking and oversight activities have experience or receive training.	Yes	According to EOUSA officials, individuals performing contract tracking and oversight activities have experience or receive training.
Activity 1	The project team performs its activities in accordance with its documented contract tracking and oversight plans.	Yes	The project team performs its activities in accordance with its documented contract tracking and oversight plans. Several reporting mechanisms are used to monitor and control the contractor's performance, including sticking to the project schedule and reporting any problems that are encountered.
Activity 2	The project team reviews required contractor software planning documents which, when satisfactory, are used to oversee the contractor team's software engineering effort.	Yes	The project team reviews required contractor software planning documents, which provide a basis for overseeing the contractor team's software engineering efforts.
Activity 3	The project team conducts periodic reviews and interchanges with the contractor team.	Yes	There are weekly meetings and monthly written status reports between the project team and the contractor.
Activity 4	The actual cost and schedule of the contractor's software engineering effort are compared to planned schedules and budgets, and issues are identified.	Yes	Actual cost and schedule of the contractor's software engineering effort are compared to the planned costs and schedule, and issues are identified. Issues so far are primarily related to the contractor's staff getting the security clearances needed to do the work.
Activity 5	The size, critical computer resources, and technical activities associated with the contractor team's work products are tracked, and issues are identified.	Yes	The contractor provides information about the size, critical computer resources, and technical activities to the ECMS project team for tracking purposes and issue identification.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Activity 6	The project team reviews and tracks the development of the software engineering environment required to provide life-cycle support for the acquired software, and issues are identified.	Yes	The project team reviews and tracks the development of the software engineering environment.
Activity 7	Any issues found by the project team during contract tracking and oversight are recorded in the appropriate corrective action system, action is taken, and the issue is tracked to closure.	Yes	According to EOUSA officials, any issues found by the project team during contract tracking and oversight are recorded in the appropriate corrective action system, action is taken, and the issue is tracked to closure.
Activity 8	The project team ensures that changes to the software-related contractual requirements are coordinated with all affected groups and individuals, such as the contracting official, contractor, and end user.	Yes	The project team ensures that changes to the software-related contractual requirements are coordinated with all affected groups and individuals, including the administrative contracting officer's representative and end users.
Measurement 1	Measurements are made and used to determine the status of the contract tracking and oversight activities and resultant products.	Yes	Measurements are made and used by the administrative contracting officer's representative to determine the status of the contract tracking and oversight activities and resultant products.
Verification 1	Contract tracking and oversight activities are reviewed by acquisition organization management on a periodic basis.	Yes	The administrative contracting officer's representative reviews contract tracking and oversight activities on a periodic basis.
Verification 2	Contract tracking and oversight activities are reviewed by the project manager on both a periodic and event-driven basis.	Yes	The project manager, on both a periodic and an event-driven basis, reviews contract tracking and oversight activities.

Source: Key practice data from SEI; analysis and comments from GAO.

Table 12: Evaluation

Common feature	CMM key practice	Satisfied?	Comments
Commitment 1	The acquisition organization has a written policy for managing the evaluation of the acquired software products and services.	Yes	The acquisition organization has defined guidelines for testing and certifying ECMS.
Commitment 2	Responsibility for evaluation activities is designated.	Yes	Responsibility for evaluation activities is designated to the ECMS project team.
Ability 1	A group that is responsible for planning, managing, and performing evaluation activities for the project exists.	Yes	The ECMS project team is responsible for planning, managing, and performing evaluation activities for the project.
Ability 2	Adequate resources are provided for evaluation activities.	Yes	According to EOUSA officials, the evaluation activities have been budgeted.
Ability 3	Individuals performing evaluation activities have experience or receive training.	Yes	Individuals performing evaluation activities have experience or receive training. The contractors were required to submit resumes along with their proposals.
Ability 4	Members of the project team and groups supporting the software acquisition receive orientation on the objectives of the evaluation approach.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Activity 1	The project team performs its activities in accordance with its documented evaluation plans.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed
Activity 2	The project's evaluation requirements are developed in conjunction with the development of the system or software technical requirements.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Activity 3	The project's evaluation activities are planned to minimize duplication and take advantage of all evaluation results, where appropriate.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Activity 4	The project team appraises the contractor team's performance over the full period of the contract for compliance with requirements.	Yes	The project team assesses the contractor team's performance continuously.
Activity 5	Planned evaluations are performed on the evolving software products and services prior to acceptance and operational use.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Activity 6	Results of the evaluations are analyzed and compared with the contract's requirements to establish an objective basis to support the decision to accept the products and services or to take further action.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Measurement 1	Measurements are made and used to determine the status of the evaluation activities and resultant products.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.

(Continued From Previous Page)

Common feature	CMM key practice	Satisfied?	Comments
Verification 1	Evaluation activities are reviewed by acquisition organization management on a periodic basis.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.
Verification 2	Evaluation activities are reviewed by the project manager on both a periodic and an event-driven basis.	No	Because of ECMS's stage in the life cycle (design phase), this key practice has not yet been addressed.

Source: Key practice data from SEI; analysis and comments from GAO.

Comments from the Department of Justice

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Justice

Executive Office for United States Attorneys
Office of the Director

Main Justice Building, Room 2616
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

(202) 514-2121

June 16, 2003

Mr. Randolph C. Hite
Director
Information Technology Architecture and Systems
U.S. General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Hite:

SUBJECT: EOUSA Response to GAO Audit Findings (GAO-03-751)

The Executive Office for United States Attorneys (EOUSA) appreciates the opportunity to comment on GAO's report (GAO-03-751). "GAO was asked to determine the extent to which EOUSA has institutionalized key IT management capabilities..." and focused on Enterprise Architecture (EA), Information Technology Investment Management (ITIM), Information Security, and System Acquisition. We disagree with the finding that the institutionalization of these key IT management capabilities are not priorities of EOUSA and the Department of Justice and, in particular, take exception with the finding that information security is not an agency priority. We believe that EOUSA has made tremendous progress in insitutionalizing these key IT management capabilities and as detailed by this report has met a majority of the key elements of each.

See comment 1.

See comment 2.

EOUSA is responsible for the management of information technology on behalf of the United States Attorneys and operates as a component of the DOJ-wide IT infrastructure in compliance with the Department of Justice's policies and procedures. EOUSA has several IT staffs dedicated to working with the Department on policy development and information technology systems. We believe it is important to note that the EOUSA Office of Chief Information Officer (OCIO) was established in January 2001 and since then has expanded to include one additional staff to support and manage Information Systems Security.

See comment 3.

FINDING: **EOUSA Has Yet to Institutionalize Key IT Management Disciplines.** "The office has defined and implemented each of the four IT management disciplines mentioned above to some degree. However, none has been institutionalized; they are not fully defined in accordance with best practices, and what has been defined has not yet been fully implemented. While these disciplines have been given attention since the recent appointment of the CIO, they have not been designated as priorities, and action plans needed for successful institutionalization have not been developed. As a result, EOUSA is currently limited in its ability to meet Justice's strategic goal of improving its IT systems, and the USAOs will be challenged in their ability to effectively and efficiently meet their mission goals and priorities."

RESPONSE:

See comment 4.

We disagree with the opinion of the team that "... EOUSA is currently limited in its ability to meet Justice's strategic goal of improving its IT systems, and the USAOs will be challenged in their ability to effectively and efficiently meet their mission goals and priorities."

See comment 5.

See comment 6.

See comment 7.

See comment 8.

The IT program of the United States Attorneys has received the highest level of support of the Department of Justice (DOJ). With the allocation of a senior level position in 2001, DOJ recognized the critical role of United States Attorneys. Since that time, EOUSA is the first DOJ component to publish an Information Technology Strategic Plan; an Enterprise Architecture; and institute an Information Technology Investment Management plan. EOUSA has been successful in gaining Level III software maturity model for its applications development process; it has insitutionalized an active Information Security program and has put its ITIM process under configuration management. We believe the finding that these processes are not a priority for this organization is unfair. EOUSA and the USAOs are viewed as leaders within the Department of Justice and senior management is very committed to the success of our IT program. Likewise, the USAOs, are leaders in the law enforcement community and effectively meet their mission goals and priorities.

2

FINDING: Enterprise Architecture: EOUSA is Not Performing Important Practices Associated with Effective Enterprise Architecture Management

RESPONSE:

See comment 9.

We agree with the finding in this area and acknowledgement our accomplishment of 80% of the elements of the GAO EA maturity framework.

EOUSA will work to implement the remaining 5 elements that consist of written polices and the formal establishment of sterring committees. In May 2002 the OCIO published the very first Enterprise Architecture for the USAOs that describes the "as is" and "to be" environment. Senior EOUSA management approved the EA and submitted it to the Department's Chief Information Officer (CIO) for approval. The DOJ CIO approved the USAOs EA in December 2002. The EA is maintained in the Department's EAMS. At the same time the department launched an initiative to develop a department-wide EA. EOUSA welcomed this opportunity and designated a chief architect to participate in the departmental working group charged with developing the new version of the EA for the DOJ. The chief architect was tasked with ensuring that USAOs EA is considered when developing the new EA. EOUSA did not "suspend its EA effort,"instead, EOUSA is actively participating in the EA Project of the entire Department of Justice, ensuring that our EA is consistent with the other agencies of the Department.

See comment 10.

FINDING: EOUSA Has Not Established Key Capabilities Needed to Effectively Manage IT Investments

RESPONSE:

See comment 11.

EOUSA agrees with GAO's finding that a selection process has not yet been used, with the following caveat that EOUSA has not engaged in any new initiatives meeting IRB review requirements since March 2003 when the IRB was put in place.

EOUSA published its first ITIM in May 2002. After review and approval by senior management, EOUSA established an Investment Review Board (IRB) and conducted its first session in March 2003. At that session, the IRB was fully trained on the investment review process, reviewed four programs/projects currently underway (the Enterprise Case Management System, Voice over IP, Victim Notification, and IT Security), and reviewed the project rating and ranking criteria and process.

3

In its current state, EOUSA ITIM meets 3 out of 5 elements of stage two of the GAO's ITIM maturity framework. The remaining 2 elements will be achieved this year by defining more detailed policies and procedures to address IT project oversight and IT project and system identification.

FINDING: EOUSA Has Not Implemented Effective Security Practices

RESPONSE:

See comment 12.
See comment 13.
See comment 14.

We do not agree with this finding. EOUSA has one of the strongest security programs within the Department of Justice and perhaps the federal government. The data of the United States Attorneys has never been comprised and is monitored on a 24x7x365 basis.

See comment 15.

We strongly disagree with the finding of GAO that " security has not been an agency priority." Security has been and continues to be a high priority of the Department of Justice leadership and EOUSA management. Since the establishment of the new position OCIO has implemented the following security projects:

See comment 16.

1. Replacement of the old virtual private network (VPN)
2. Implementation of the largest (24x7x365) intrusion detection system (IDS) within DOJ[1]
3. Secure Remote Access for Dial-up connection
4. Certification and Accreditation of more than 8 systems
5. Implementation of virus detectors on all hardware devices
6. Real-time encryption of all data in laptops and handheld devices
7. Use of proximity sensors for equipment used in common areas
8. Vulnerability assessment
9. Penetration testing
10. More than 223 security CERT risk analysis have been reviewed during the past six months

There are more examples of EOUSA's commitment to the security of our IT resources, including the allocation of 10 additional security positions for the districts and two additional FTEs to the Information Systems Security Office.

See comment 17.

[1] GAO recommended the implementation of an IDS solution. EOUSA has an IDS in place for all of its offices; however, EOUSA does not have the authority to implement an IDS for the wide area network. The Justice Consolidated network is managed, secured, and monitored by the department and Sprint.

See comment 18.

See comment 19.

See comment 20.

See comment 21.

See comment 22.

See comment 23.

See comment 24.

See comment 25.

The Department of Justice Inspector General conducted a security audit of several USAOs last year and they found ten vulnerabilities in those offices. All but one of those findings have been resolved, the last being related to our outdated VPN and review of the audit logs. From a practical standpoint, it does not make sense to invest in a costly and time consuming risk assessment of the old VPN when it will be completely replaced by the end of July 2003.

To declare our risk assessment program inadequate due to one outgoing system not having a formal, documented risk assessment is an over-generalization. We perform formal facilitated risk assessments on every system and additionally an automated quantitative assessment on all major systems. Also, a project is underway to implement automated tools to review audit logs, as we do not have the resources to analyze the mass amount of data generated by audit logs. Regular tests will be conducted to determine the compliance of information technology systems with policies and procedures.

EOUSA does have plans in place to address security issues. In accordance with Government Information Security Reform Act (GISRA) requirements, we have a plan of action and milestones for weaknesses identified during Certification and Accreditation (C&A). We also have contingency plans for all C&A'd systems, which are tested prior to certification. We are currently engaged in annual testing of contingency plans. Our C&A certification testing is based on DOJ Order 2640.2D.

EOUSA is also working with the Department to implement a centralized security training program for all users within the USAOs. This training program will be in place before the end of August 2003.

FINDING: EOUSA Is Employing Important Acquisition Management Practices on a Key System

We agree with these findings as noted herein. The system that was reviewed for acquisition strategy is still under development. The Enterprise Case Management System follows a very rigorous System Development Lifecycle Methodology (SDLC); however, it is not the first development effort to follow the SDLC. Even at its current stage of development, GAO reports that ECMS meets 80 out of 94 elements of the Level 2 of SEI's Software Acquisition Capability Maturity Model.

5

See comment 26.

See comment 27.

EOUSA is committed to a mature software development environment. The LIONS application, which is currently in production, was certified at SEI Capability Maturity Model Level-III by an independent vendor. The news of this success will soon be published in Government Computer News and Federal Computer Weekly.

It should be noted that EOUSA acquisitions are all processed through the Department and must comply with all Departmental policies and procedures. EOUSA did not develop separate acquisition policies; however, GAO's recommendations will be implemented and additional policies will be developed for oversight and contract tracking.

In conclusion, I thank the members of the team that worked with us in this audit. We are fully committed to supporting the mission and strategies of the Department of Justice and support of the United States Attorneys' offices. I believe that the accomplishments of our Information Technology Staff are noteworthy and they serve as a model for the Department of Justice. We will continue to work to improve our processes and our systems and thank you again for the opportunity to comment on this report.

Sincerely,

Guy A. Lewis
Director

cc: Vickie Sloan
Director, Audit Liaison Office

6

The following are GAO's comments on the Department of Justice's letter dated June 16, 2003.

GAO Comments

1. We disagree. Our position that institutionalization has not been a priority is based on two facts that EOUSA did not dispute: (1) plans for addressing the weaknesses cited in our report do not exist and (2) limitations in resources to address these weaknesses were cited by EOUSA officials as the reason why the weaknesses exist. If each of these areas were an agency priority, then plans would be in place to address the weaknesses, and resources to execute the plans would be committed.

2. We do not question EOUSA's statement that it has made "tremendous progress." Our work focused on determining the extent to which EOUSA currently satisfies key practices in the four IT management disciplines. It did not include developing a baseline from which to measure progress. To EOUSA's credit, our review showed that the office has satisfied many key practices in each discipline, and we have noted this in our report.

3. We agree and include both of these facts in our report.

4. We disagree. EOUSA's comments did not include any information to refute our conclusion. Given that it did not have a plan for fully implementing best practices for each discipline, and had not allocated adequate resources to support such a plan, we have not modified our conclusion.

5. We do not question these statements about the position of EOUSA and the USAOs relative to other Justice components. Such a comparison was not part of the scope of our work.

6. We disagree. EOUSA has not gained this maturity level. Rather, according to EOUSA, the contractor that maintains its LIONS application is certified as a level 3 software developer. In contrast, our work focused on EOUSA's capabilities as a software acquirer, and thus addresses a different organization, discipline, and maturity model.

7. See comment 1.

8. We do not question this statement because the position of EOUSA and the USAOs relative to other Justice components or other law enforcement entities was not part of the scope of our work.

9. As noted in our report, EOUSA satisfied about 80 percent of the elements of just *stage 2* of the EA management framework. It has satisfied about 60 percent of the elements (12 out of 19) of the entire framework.

10. We have modified the report to reflect this comment.

11. We agree. However, according to GAO's IT Investment Management Framework, to satisfy the proposal selection critical process, EOUSA would need to demonstrate the use of the criteria it has defined. Because it has not yet done so, it is not satisfying the critical process and thus has met two out of five elements of stage 2 of the framework.

12. We disagree. Our assessment is based on EOUSA's satisfaction of key practices laid out in our executive guide for information security management.[1] This assessment showed that EOUSA has not fully satisfied any of these key practices. For example, EOUSA does not (1) have a central security focal point with appropriate resources, (2) adequately promote user awareness, and (3) regularly monitor the effectiveness of security controls. Until EOUSA addresses these and other security weaknesses we identify in our report, it will not have implemented effective security practices.

13. See comment 8.

14. We do not question this statement because determining whether the data of the United States Attorneys have never been compromised and are monitored 24 hours a day, 7 days a week was not within the scope of our work and EOUSA did not provide any evidence supporting its assertions.

15. See comment 1. Additionally, our finding is that the *institutionalization* of information security management has not been an agency priority.

[1] U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

16. We do not question these security initiatives. Additionally, we emphasize that our message is not that EOUSA has not taken steps to improve its information security posture, but rather that the office's information security management efforts, including ongoing and completed improvement steps, are weak in a number of areas relative to information security management best practices.

17. We agree, but would add that our recommendation could be addressed by actively monitoring activity at the routers, firewalls, and wide area network devices, which we understand are remotely managed by EOUSA. To avoid any potential confusion on this point, we have clarified our recommendation. Implementing an intrusion detection system to monitor activity at the routers, firewalls, and other network devices would enable EOUSA to detect hostile attempts to manage those devices.

18. We do not question EOUSA's statement that it has been working to resolve vulnerabilities identified during a security audit conducted by the Justice Inspector General. The scope of the Inspector General's audit, however, was narrower than ours in that it focused on EOUSA's local area network environment.

19. We agree that given EOUSA's recent progress in deploying the replacement network its exposure to risk is currently limited. We have modified the security risk assessment section of the report and the associated recommendation to reflect this change in circumstances.

20. We agree and thus do not conclude that EOUSA's risk assessment program is inadequate. Rather, based on the fact that a risk assessment was not performed on the network that EOUSA has operated since 1996 and, until recently, relied exclusively on, we conclude that EOUSA has not always performed risk assessments. Additionally, to recognize the recent change in circumstances we have modified our recommendation concerning risk assessments.

21. We do not question these statements. We support the use of automated tools to review audit logs, particularly because these logs were not being reviewed, and EOUSA attributed this to a lack of resources. We also support EOUSA's plan to conduct regular tests to determine compliance with policies and procedures. Both of these planned actions are consistent with our recommendations.

22. We do not question this statement. However, as noted in our report, the office did not have a plan to address the issues that are discussed in our report.

23. We do not question these statements because our review did not address contingency plans for all certified and accredited systems. As stated in the report, while a contingency plan was developed for the replacement network, it was not prepared in accordance with federal guidelines. For example, the plan did not specify procedures for notifying recovery personnel. To clarify our position, we have added examples to the report of this plan's noncompliance with federal guidelines.

24. We support EOUSA's stated commitment to establish a centralized security training program. Establishing such a program is consistent with our recommendations.

25. We have modified the report to reflect that the Enterprise Case Management System is the first acquisition to follow the Justice life-cycle methodology from its inception.

26. See comment 6.

27. We have modified the report to reflect that EOUSA's acquisitions are processed through the department and must comply with all departmental policies and procedures.

GAO Contact and Staff Acknowledgments

GAO Contact

Lester P. Diamond, (202) 512-7957

Acknowledgments

In addition to the individual named above, Nabajyoti Barkakati, Jamey Collins, Joanne Fiorino, Anh Q. Le, Sabine R. Paul, and William F. Wadsworth made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

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

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

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00