United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations, House of Representatives

September 1989

JUSTICE AUTOMATION

Security Risk Analyses and Plans for Project EAGLE Not Yet Prepared

RESTRICTED——Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations.

GAO/IMTEC-89-65

GAO

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

Information Management and
Technology Division

B-233809

September 19, 1989

The Honorable Bob Wise
Chairman, Subcommittee on Government Information,
Justice, and Agriculture
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

In a July 28, 1988, request and in subsequent discussions with your office, we were asked to review various aspects of EAGLE[1] —a Department of Justice project intended to supply office automation systems to its lawyers, managers, secretaries, and other employees. The current cost of this project, for which a contract was awarded in June 1989, is $76 million.[2] On December 8, 1988, we briefed the former Chairman's office on Justice's approach to satisfy its office automation needs and whether Project EAGLE was being acquired in accordance with federal procurement policies and procedures.

While this briefing satisfied the former Chairman's request, we were asked to provide additional information on Justice's actions to ensure that information maintained in the systems acquired under Project EAGLE is properly safeguarded. Accordingly, this report provides requested information on the Department of Justice's efforts to develop security plans and conduct risk analyses for the Project EAGLE systems, as required by federal law and regulations.

Although sensitive information[3] will be contained in the Project EAGLE systems, Justice has not developed security plans or conducted risk analyses for these systems. The Computer Security Act of 1987 (PL 100-235) and other federal regulations and guidelines require that these actions be taken to ensure that the information will be protected against unauthorized access or disclosure.

[1]EAGLE stands for Enhanced Automation for the Government Legal Environment.

[2]According to Justice officials, the actual cost of the EAGLE systems may vary depending upon the extent to which Justice exercises upgrade options included in the contract.

[3]According to the definition of terms stated in the Computer Security Act of 1987 (15 U.S.C.A. 278g-3(d)(4)(West Supp. 1989)), sensitive information is any information which if lost, misused, or accessed or modified without authorization, could adversely affect the national interest or conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act (5 U.S.C. 552(a)).

During the course of our review, Justice officials stated that they intended to perform risk analyses and develop security plans after the Project EAGLE systems were installed and operating. In later discussions with these officials, we pointed out that such actions should take place prior to the systems' installation to ensure that proper safeguards are incorporated in the systems. Justice officials subsequently agreed to revise their approach and began taking steps to prepare the risk analyses and security plans prior to the installation and operation of the EAGLE systems. These steps, if properly completed prior to installing the systems in each site, should help ensure the security of these systems. Accordingly, we are making no recommendations at this time.

In performing this review, we examined Justice's policies for securing automated information resources, related security requirements, and relevant documents pertaining to the Project EAGLE procurement. We also interviewed the project manager and other Justice officials having knowledge of Project EAGLE to determine their strategy for assessing the project's security risks and identifying appropriate safeguards. Our work was performed in accordance with generally accepted government auditing standards from August 1988 to June 1989. Additional information on our objectives, scope, and methodology is contained in appendix I.

Background

Under the direction of the Attorney General, Justice represents the government in federal legal matters that include performing investigations, conducting grand jury proceedings, and preparing and trying cases and appeals. Legal and prosecutorial functions are conducted by Justice's litigating organizations, which include 94 U.S. Attorney Offices and six divisions—Antitrust, Civil, Civil Rights, Criminal, Lands and Natural Resources, and Tax.

In response to increasingly large and complex caseloads, Justice's litigating organizations have come to rely on various incompatible office automation systems—ranging from advanced, multifunction systems in some organizations to less sophisticated, stand-alone, single-function workstations in others. As part of a study completed in 1986,[4] Justice researched alternatives to achieve a more uniform office automation capability and increase the efficiency and productivity of its litigating organizations. Justice concluded that it would benefit most from an

[4]U.S. Department of Justice, Uniform Office Automation and Case Management Project - Phase I Report, Mar. 26, 1986.

office automation system that would provide interoperability (that is, the ability to communicate through an interface) among the incompatible systems in the litigating organizations in the short-term, and uniform hardware and software among these and other departmental systems in the long-term.

To accomplish these objectives, Justice initiated in May 1986 design and development activities, which ultimately led to the award of an 8-year, $76 million contract for Project EAGLE. Under the contract, which was awarded in June 1989, Justice plans to acquire hardware, commercial off-the-shelf software, and essential support services (such as maintenance and training) to meet its office automation and information management requirements.

The Project EAGLE contract is expected to provide a network of integrated systems, linking 12,000 workstations in 200 sites nationwide. The project is designed to enable users to perform on one workstation a variety of functions that currently must be performed on multiple, standalone, single-function terminals. These functions include word processing, data base management, document storage and retrieval, electronic mail, and calendar management. In addition, the EAGLE systems should provide all users with desktop access to a variety of other systems and services, such as existing case management and litigation support systems, on-line legal research services, and Justice Data Center operations.

Justice initially plans to install EAGLE systems in three of its litigating organizations—the Tax Division, Criminal Division, and U.S. Attorney Offices. Also, to achieve departmentwide, uniform office automation, other litigating and nonlitigating organizations will be required to either purchase EAGLE hardware and software or acquire systems that are compatible with Project EAGLE.

Justice had planned to begin installing the EAGLE workstations within 60 days after the contract was awarded, and to complete the installations in about 3 years. However, these plans were put on hold in late June 1989 after three vendors that unsuccessfully bid on the contract protested the award. According to the EAGLE project manager, these protests have since been resolved and Justice now plans to begin installing the workstations in late October 1989.

Because the EAGLE systems will contain sensitive information—including the names of defendants, witnesses, informants, and undercover law enforcement officials—this project is subject to the requirements of the

Computer Security Act of 1987 and other applicable federal guidelines and regulations. The Computer Security Act of 1987 requires federal agencies to identify, and develop security plans for, operational and developmental computer systems that contain sensitive information.[5] Office of Management and Budget (OMB) guidelines stipulate that each plan must include a basic description of the purpose, environment, and sensitivity of the system; the system's security and privacy requirements; and the agency's plan for meeting those requirements.[6] The Federal Information Resources Management Regulation (41 C.F.R. part 201-7) and OMB policies[7] further require agencies to conduct a security risk analysis to assess the threats to which the system will be exposed and the vulnerabilities of the system before its operational use.

Security Plans and Risk Analyses Not Prepared for Project EAGLE

Justice has not developed security plans or performed security risk analyses for Project EAGLE to ensure that sensitive information contained in the systems will be adequately protected. The EAGLE project manager and other officials in the Justice Management Division recognized the requirement for such actions, but prior to discussing these issues with us had not intended to conduct risk analyses or prepare security plans until after the systems were installed and operating.

The officials cited two reasons for this position. First, they believed existing physical security safeguards (such as building and computer room access controls) were adequate for the time being and that any refinements could be made after the systems' installation. Second, they contended that system security needs could not be determined because the systems' architecture, including hardware and software requirements, was unknown prior to selecting the winning vendor. The Request for Proposals specified the functional requirements and performance criteria for the systems but allowed vendors to propose the architecture, equipment, and software.

In discussions with these officials, we expressed concerns with the reasons they cited for not conducting the risk analyses and developing the security plans prior to the systems' installation. With regard to their position on physical security, we pointed out that such safeguards alone

[5]40 U.S.C.A. 759nt. (West Supp. 1989).

[6]Office of Management and Budget Bulletin No. 88-16, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information, July 6, 1988.

[7]Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, Dec. 12, 1985.

are not the only controls that are necessary to ensure adequate protection of the data processed and maintained within the systems. Typically, systems such as those included in Project EAGLE require operational and technical controls, as well as physical controls. Operational controls include, for example, the formulation of contingency plans for backup in the event of a system failure. Technical controls include authenticating the identity of remote users, and encryption of data during transmission.

Regarding the officials' contention that the systems' architecture was unknown, we noted that with the award of the Project EAGLE contract in June 1989, the architecture, including the hardware and software requirements, should now be available. The contract specified the types and quantities of hardware and software that will be required to meet Justice's office automation needs.

In light of the above, we see no compelling reason for Justice to delay conducting risk analyses and preparing security plans until after the Project EAGLE systems are installed. As we reported in May 1988, the most efficient and effective means to ensure that a system contains appropriate security controls is to address security issues when designing the system, not after it is installed.[8] Given that the contract has been awarded and the systems' architecture has been determined, Justice's emphasis should now be on performing these tasks as early as possible. To ensure that proper safeguards are incorporated in these systems in accordance with applicable federal requirements, the analyses and plans should be completed prior to installation and use.

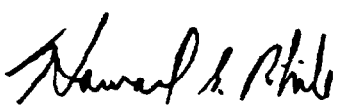
After discussing our concerns with Justice officials, they agreed to perform risk analyses and prepare security plans before installing and operating the EAGLE systems. The Director of the Justice Management Division's Systems Policy Staff agreed that performing risk analyses prior to installing equipment will better ensure that security threats are identified and needed safeguards are implemented. The EAGLE project manager stated that Justice has the opportunity to perform the risk analyses on a site-by-site basis prior to installing the hardware and software being procured under this contract. He added that Justice has begun developing guidelines for conducting risk analyses and preparing security plans for those sites that will acquire the EAGLE systems. The guidelines are due to be completed in early October 1989. We believe

[8]Information Systems: Agencies Overlook Security Controls During Development (GAO/IMTEC-88-11) May 31, 1988.

these actions, if properly completed prior to installing the systems in each site, should help ensure the security of these systems. Accordingly, we are making no recommendations at this time.

As requested by your office, we did not obtain formal agency comments on this report. However, we discussed the information in the report with responsible Justice officials and have included their comments where appropriate. As agreed with your office, unless you publicly announce the report's contents earlier, we plan no further distribution until 30 days from the date of the report. At that time, we will send copies to the Attorney General of the United States and other interested parties. This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who may be reached at (202) 275-3455. Other major contributors are listed in appendix II.

Sincerely yours,



for Ralph V. Carlone
Assistant Comptroller General

Contents

Abbreviations

EAGLE	Enhanced Automation for the Government Legal Environment
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
OMB	Office of Management and Budget

Objectives, Scope, and Methodology

In a July 28, 1988, letter and in subsequent discussions with the Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, we were asked to review various aspects of Project EAGLE, a major initiative to supply office automation systems within the Department of Justice. During a December 8, 1988, meeting, we briefed the former Chairman's office on Justice's approach for satisfying its office automation needs and the extent that Justice is complying with federal procurement policies and procedures to acquire Project EAGLE. Although this briefing satisfied the former Chairman's request, we were asked to provide additional information on Justice's efforts to ensure that information contained in the Project EAGLE systems is adequately protected. In particular, we were asked to examine Justice's efforts to conduct risk analyses and prepare security plans for the systems acquired under Project EAGLE, as required by federal law and regulations.

To assess Justice's efforts to conduct risk analyses and prepare security plans for Project EAGLE, we identified and reviewed the policies and procedures under which Justice manages and secures its computer systems containing sensitive information. We compared Justice's procedures to the Computer Security Act of 1987 and federal regulations guiding the security of information resource systems. To identify security provisions currently planned for the systems, we reviewed requirements specified in the Project EAGLE Request for Proposals and the awarded contract. We also interviewed the EAGLE project manager and policy and oversight staff in the Justice Management Division regarding Justice's actions and strategy for assessing Project EAGLE's security risks and identifying necessary safeguards.

To understand the overall objective and approach for acquiring Project EAGLE, we identified and reviewed Justice's automated information systems strategic planning documents and its uniform office automation study. We interviewed members of the Project EAGLE steering committee and discussed the overall procurement strategy with oversight staff at the Office of Management and Budget.

We performed our work between August 1988 and June 1989 at the Department of Justice headquarters in Washington, D.C. Our work was performed in accordance with generally accepted government auditing standards. As requested by your office, we did not obtain official agency comments on a draft of this report. However, we discussed the information in this report with Justice officials and have included their comments where appropriate.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.

James R. Watts, Associate Director
Joseph T. McDermott, Assistant Director
Valerie C. Monroe, Evaluator-in-Charge
Colleen M. Phillips, Evaluator
Steven Merritt, Technical Adviser

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100