United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
10:00 a.m. EDT
Thursday
June 27, 1991

Serious Questions Remain About Justice's Management of ADP and Computer Security

Statement of
Milton J. Socolar
Special Assistant to the Comptroller General

Before the
Subcommittee on Economic and Commercial Law
Committee on the Judiciary
House of Representatives

B-238836

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to share our perspectives on how well the Department of Justice is managing its automated data processing (ADP) resources and its computer security. We have found serious problems in both areas.

In today's world, the ability of an organization to manage and secure its information resources is more than a desirable extra: it is essential to doing business effectively. Until Justice gains control over these areas, congressional trust that the Department can effectively, efficiently, and securely handle modern technological resources in carrying out its important mission will remain in doubt.

Indeed, senior Justice officials themselves acknowledge that they have not effectively fulfilled their ADP management responsibilities--a matter of particular concern in light of the Department's plans to spend over $2.7 billion for information technology and related services between fiscal years 1991 and 1995.

ADP MANAGEMENT

In brief, Mr. Chairman, while the Assistant Attorney General for Administration will today relate steps that the Department--and the Justice Management Division in particular--have taken to more adequately address these shortcomings, such steps to date are mainly organizational and structural; they may well be insufficient to solve the pervasive problems that have plagued Justice's information resources management (IRM) program for over a decade. Serious questions remain concerning whether these changes will translate into establishing the leadership required.

In testimony before the full Judiciary Committee last fall--and in a companion report--we detailed Justice's persistent and long standing problems in ADP management, and its repeatedly inadequate responses to our recommendations for improvement.[1] At that time we discussed the fact that after a number of false starts over a decade, Justice still does not have a system that accurately provides the total number of cases being litigated and the total number of staff in the litigating organizations working on them. We also discussed the lack of a comprehensive IRM plan to assist in managing Justice's information resources, and the absence of a senior IRM official with clear authority to require component organizations to implement Departmentwide IRM decisions.

---

[1] Problems Persist in Justice's ADP Management and Organizations (GAO/T-IMTEC-91-2, Dec. 5, 1990) and Information Resources: Problems Persist in Justice's ADP Management and Operations (GAO/IMTEC-91-4, Nov. 6, 1990).

In addition, we related Justice's own acknowledgment that it did not have sufficient staff with adequate technical and managerial capabilities to conduct large-scale ADP acquisitions and provide the required oversight. For example, although the central IRM office reviews information systems plans and acquisition lists from Justice's component organizations, staff shortages at the central IRM office have prohibited independent audit and evaluation of computer systems, according to officials of that office. As similarly reported in September 1990, the Department's Immigration and Naturalization Service risks admitting illegal aliens and granting benefits to ineligible aliens--and has millions of dollars in uncollected debts--because of unreliable ADP systems.[2] According to Justice, limited resources prevented it from conducting comprehensive oversight of the Service's information management program.

In its April 1991 response to our November 1990 report, Justice stated that the Department had just created the position of Deputy Assistant Attorney General for Information Resources Management, restructured the Justice Management Division, and taken other steps to create an effective IRM program. These actions are steps in the right direction. However, these changes, in our view, are insufficient to solve the serious and pervasive problems that have plagued the Justice IRM program for over a decade. The Department's response to our November 1990 report failed to address our recommendations that the Attorney General

-- require the case management system to have uniform, accurate, and complete case information;

-- require development of an IRM plan;

-- clarify the senior IRM official's authority in implementing departmentwide IRM decisions; and

-- augment, where necessary, central IRM office capabilities in the technical and management areas, ADP contract management, and oversight.

Last week we met with senior Justice officials to find out exactly what steps the Department had taken to address our recommendations. As a result of that meeting, we learned that the Department

---

[2]Information Management: Immigration and Naturalization Service Lacks Ready Access to Essential Data (GAO/IMTEC-90-75, Sept. 27, 1990).

-- contracted in August 1990 with FEDSIM, an organization within the General Services Administration, to do a requirements analysis for the purpose of developing a case management system that provides uniform, accurate, and complete case information;[3]

-- is developing its IRM plan to be finalized within the next few months;

-- has augmented central IRM office capabilities in the areas of technical and management, ADP contract management, and oversight by assigning additional staff and filling the position of Deputy Assistant Attorney General for Information Resources Management; and

-- issued a memorandum on June 20, 1991, to the heads of all components clarifying the senior IRM official's authority in implementing departmentwide IRM decisions.

These efforts are good, important beginnings. But, dedicated, focused, Departmentwide leadership and sustained oversight will be required to complete these initiatives and bring about real change. For example, FEDSIM is not expected to complete its requirements analysis for the case management system until the end of this calendar year--and it will be 3 years before the Department will have a complete case management system in operation.

COMPUTER SECURITY

Mr. Chairman, at this hour one of my colleagues is testifying on the Department's computer security weaknesses before another committee.[4] While part of overall ADP management, the requirement for computer security deserves special attention. Serious security vulnerabilities remain--vulnerabilities that have life-or-death implications.

As you know, the Computer Security Act of 1987 requires federal agencies to develop security plans for computer systems that they designate as containing sensitive information, and to establish mandatory computer security training to make employees aware of their specific responsibilities and how to fulfill them. The Federal Information Resources Management Regulation (41 C.F.R.

---

[3]FEDSIM stands for Federal Computer Performance Evaluation And Simulation Center and specializes in performing technical evaluations.

[4]Computer Security Weaknesses at the Department of Justice (GAO/T-IMTEC-91-15, June 27, 1991).

part 201-7) and Office of Management and Budget (OMB) instructions direct agencies to protect access to and operation of computer systems by conducting risk analyses and preparing and testing contingency plans. Nevertheless, Mr. Chairman, last year we found that the Justice Management Division was not ensuring that the Department's highly sensitive computer systems were adequately protected.[5]

For example, we found several material weaknesses in physical and other operational security at the Justice main data center. Justice processes sensitive information at this facility and plans to process classified information there. Access to the data center was not properly controlled. An electronic card-key device that records when employees enter and exit did not record, store, or generate reports on activities of cardholders, leaving center officials unable to reconstruct events if they needed to investigate a security breach. Guards were not positioned to visually survey activities in the center. Video monitors, where used, lacked recording mechanisms to store and replay information should it be needed. Some more examples-- contingency plans to deal with service interruptions to the computer systems that process sensitive information either had not been prepared or were not tested, and mandatory computer security awareness training was not being provided to employees.

We previously testified about a Justice security breach last summer at Lexington, Kentucky.[6] Computer equipment excessed by the U.S. Attorney's Office was later found to contain highly sensitive data, including grand jury material and information regarding confidential informants. How this could have happened is disturbing in itself, but even more shocking was that it happened again. As recently as this past February, a different U.S. Attorney's office cautioned federal and local officials that, again, sensitive data that could potentially identify agents and witnesses might have been compromised.

While the highly sensitive nature of our findings in the Kentucky investigation precludes full discussion of relevant details in this public session, I can say that patterns of neglect and inattention were found nationwide--patterns that allowed the Department to compromise information that may have jeopardized the lives of those whose safety depended on anonymity.

---

[5]Justice Automation: Tighter Computer Security Needed (GAO/IMTEC-90-69, July 30, 1990).

[6]Justice's Weak ADP Security Compromises Sensitive Data (Public Version) (GAO/T-IMTEC-91-6, Mar. 21, 1991).

We recommended that the Attorney General immediately

-- identify all surplused equipment;

-- determine whether or not such equipment might have contained sensitive data; and

-- prepare a damage assessment of the impact that such compromised information would have on carrying out its mission and on the identity of witnesses, confidential informants, and undercover agents.

We also recommended that the Attorney General (1) strengthen the Justice Management Division's leadership and oversight of Departmental computer security programs, and (2) report the computer security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act. We further recommended that OMB designate computer security at the Department of Justice as a high-risk area.

To its credit, Justice has taken some steps--and plans more--to improve the security of its computer systems and its sensitive information. In March of this year, the Department acknowledged the need for improved computer security and identified efforts either planned or underway to address the agency's computer security deficiencies. These actions include (1) a more active leadership role on the part of the Department's security staff in the Justice Management Division, (2) a major security upgrade of the Department's data center, and (3) increased security awareness training.

This past April the Attorney General directed the heads of Department components to immediately review their security programs. And last month, the Assistant Attorney General for Administration directed component heads to provide him their plans to ensure that all Justice employees receive mandatory computer security awareness training by November 1, 1991. In addition, the Department notified OMB on June 20, 1991, that they intend to designate computer security as a material internal control weakness in the Department's 1991 Financial Integrity Act report.

No action, however, had been taken by the Department as of last week to identify all surplused computer equipment and determine whether any sensitive data was involved. But, we were told a few days ago by senior Justice officials that there will be a follow up on computer equipment surplused throughout the Department during the last 18 months.

PROJECT EAGLE

Mr. Chairman, I would also like to address another matter that has caused concern--the Department's procurement and management of its Project EAGLE network. The project is designed to enable each user to perform at his or her workstation a variety of functions, such as word processing, data base management, and document storage and retrieval.

In 1989 we found that although highly sensitive information such as the names of witnesses and undercover agents would be contained in the Project EAGLE network, Justice had not developed security plans or conducted risk analyses for the systems.[7] The EAGLE network is composed of integrated sub-systems with 12,000 workstations at 200 sites nationwide processing sensitive information such as the names of undercover agents and witnesses. As previously mentioned, federal regulations and OMB policies require that agencies conduct risk analyses to identify areas of vulnerability and prepare and test contingency plans. Justice was going to wait until after Project EAGLE was installed and operational before performing the required risk analyses or developing security plans. After we took issue with this approach, Justice officials agreed to prepare the security analyses and plans prior to the installation and operation of the system.

Our recent preliminary followup work shows that some improvements have been made. Nevertheless, risk analyses are still not being completed before installation at some locations and all vulnerabilities identified by the risk analyses that have been performed are not being corrected expeditiously.

Finally, I would mention that we have also been troubled by the Department's response to protests of its EAGLE procurement. The Department sanctioned a settlement pursuant to which the contract awardee agreed to pay significant sums to the protesters and the Department agreed to pay the awardee $200 thousand as a contribution toward the settlement costs. Settlements like this to avoid the issue as to whether or not proper procurement procedure was followed effectively thwart the objective of the protest process to identify and correct illegal agency actions.

- - - - -

[7] Justice Automation: Security Risk Analyses and Plans for Project EAGLE Not Yet Prepared (GAO/IMTEC-89-65, Sept. 19, 1989). EAGLE stands for Enhanced Automation for the Government Legal Environment.

In summary Mr. Chairman, the Department has serious problems in managing its information technology resources and providing adequate security for its computer systems. While the Department has already taken some positive steps to address these problems, and has told us of plans to do more, we do not know how effective such actions will be, especially since Justice has experienced many false starts in the past. Therefore, continuing oversight by the Congress and by top Justice management will be required to bring about any real change.

This concludes my statement, Mr. Chairman. I would be pleased to respond to any questions you or other Members of the Subcommittee may have at this time.