United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
9:30 p.m. EDT
Thursday
June 27, 1991

Computer Security Weaknesses at the Department of Justice

Statement of
Howard G. Rhile
Director, General Government Information Systems
Information Management and Technology Division

Before the
Subcommittee on Technology and Competitiveness
Committee on Science, Space, and Technology
House of Representatives

B-233809

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our work in the area of computer security at the Department of Justice. The Department relies on computer systems to process highly sensitive information, including the names of defendants, witnesses, informants, and undercover law enforcement officials. The dependence on computer systems to process sensitive information presents considerable risk. If the systems and/or Justice employees fail to protect this information from unauthorized access and disclosure, individuals could be harmed and public trust eroded.

Our work over the past 3 years for the Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, identified many disturbing weaknesses in Justice's implementation of the Computer Security Act of 1987 and applicable regulations. The weaknesses we identified have life-and-death implications for individuals whose identities may have been compromised because of inadequate control over sensitive information contained in the Department's computer systems.

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. part 201-7) and Office of Management and Budget policies further direct agencies to protect access to and operation of computer systems by requiring that agencies (1) conduct risk analyses to identify areas of vulnerability, and (2) prepare and test contingency plans.

The fact remains, Mr. Chairman, that the Department of Justice has not been ensuring that its highly sensitive computer systems are protected. Recognizing its vulnerability and the need to improve its computer security status, the Department is now taking more of a leadership role. In recent months, the Department has taken a number of actions designed to address its computer security deficiencies.

SENSITIVE COMPUTER SYSTEMS FOUND VULNERABLE

In 1989 we found that, although highly sensitive information will be contained in the Project EAGLE systems, Justice had not developed security plans or conducted risk analyses for these systems.[1] The EAGLE network is composed of integrated systems

---

[1]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.

with 12,000 workstations in 200 sites nationwide processing sensitive information, such as the names of defendants and witnesses. Justice was going to wait until after the Project EAGLE systems were installed and operational before performing the required risk analyses or developing security plans. After we took issue with this approach, however, Justice officials agreed to prepare the security analyses and security plans prior to the installation and operation of the EAGLE systems. Our recent preliminary followup work shows that some improvements have been made. Nevertheless, risk analyses are still not being completed before installation of the systems in some locations and all vulnerabilities identified by risk analyses that have been done are not being corrected expeditiously. Moreover, Justice is still finalizing its security plan for the EAGLE systems.

In 1990 we found that Justice was not ensuring that its highly sensitive computer systems were adequately protected. We identified many disturbing weaknesses in existing security that could severely compromise both the computer systems and the sensitive information they process. We reported that these weaknesses reflected inadequate leadership and oversight by the Justice Management Division, which is responsible for developing and directing the Department's computer security programs. Within Justice's seven litigating organizations, for example, we found that contingency plans necessary to combat service

interruptions to the computer systems used to process sensitive information either had not been prepared or were not tested.[2] Further, no mandatory computer security training was being provided to employees.[3]

During this review, we also found several material weaknesses in physical and other operational security at Justice's main data center. Justice processes sensitive information at this facility, and plans to process classified information. Our review disclosed, for example, that 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; therefore, center officials could not reconstruct these events if they needed to investigate a security breach. Further, guards were not positioned to visually survey activities in the center, and video monitors, where used, lacked recording mechanisms to store and replay information should it be needed. At present, Justice is in the process of making major security upgrades to its data center.

---

[2]Justice's litigating organizations include 94 U.S. Attorney's Offices and six divisions--Antitrust, Civil, Civil Rights, Criminal, Land and Natural Resources, and Tax.

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

Just 3 months ago we testified about yet another example of inadequate computer security at the Department of Justice.[4] We reported the results of our investigation of last summer's security breach in Lexington, Kentucky, in which 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 happen is shocking in itself, but even more dangerous was Justice's ongoing vulnerability. 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.

Mr. Chairman, the highly sensitive nature of our Kentucky investigation's findings precludes us from being able to fully describe in open session all of the details of what we uncovered. I can say, however, that we found patterns of neglect and inattention nationwide that have resulted in Justice's compromising sensitive information that could result in the possible loss of life of individuals whose identities may have been disclosed.

---

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

DECISIVE ACTION LONG OVERDUE

Our investigations since 1989 lead to the unmistakable conclusion that until Justice radically changes its approach to computer security, one cannot trust that sensitive data will be safely secured at the Department. The problems brought to light by the Kentucky incident and our other investigations are systemic--and they require dedicated, focused, Departmentwide attention to bring about the changes that must be made. Such attention must be sustained.

Our reports contained recommendations to the Attorney General to (1) ensure that the computer security weaknesses we found were properly corrected, (2) strengthen the Justice Management Division's leadership and oversight of departmental computer security programs, and (3) report the computer security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act. We further recommended that the Office of Management and Budget designate computer security at the Department of Justice as a high-risk area.

JUSTICE'S ACTIONS: A BEGINNING

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 proactive 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, (3) increased security awareness training, and (4) more aggressive oversight of the preparation and utilization of contingency plans. In addition, in April 1991, the Attorney General directed the heads of Department components to conduct immediate reviews of their security programs. And last month, the Assistant Attorney General for Administration directed component heads to provide him with their plans to ensure that all Justice employees receive mandatory computer security awareness training by November 1, 1991.

It is apparent that the Department of Justice has recognized the importance of computer security, and is beginning to take the steps necessary for improvement. However, Mr. Chairman, we do not yet know how effective the Department's actions will be. Continuing oversight by the Congress and Justice's top management will be required to sustain needed improvement.

- - - - -

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions that you or members of the Subcommittee may have at this time.