United States General Accounting Office

GAO Testimony

For Release
on Delivery
Expected at
10:00 a.m. EST
Thursday,
March 21, 1991

Justice's Weak ADP Security Compromises Sensitive Data

(PUBLIC VERSION)

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

Before the Committee on Government Operations
Subcommittee on Government Information,
Justice, and Agriculture
House of Representatives

Mr. Chairman and Members of the Subcommittee:

At your request we reviewed last August's sale of surplus Department of Justice computer equipment by the U.S. Attorney's Office in Lexington, Kentucky--equipment, it was later found, containing highly sensitive data. How this could happen and how adequately Justice has responded is an important story, one with life-and-death ramifications for individuals whose identities may have been compromised by the exposure of this sensitive information.

Even more important, however, is the Department's continuing exposure to similar breaches of security. While the Kentucky incident happened 7 months ago, as recently as last month 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 findings precludes our being able to fully describe in open session the appalling details of what we have uncovered. The Department of Justice has designated for "limited official use" reports that disclose security vulnerabilities. While this is an administrative designation, and in itself is not grounds for failing to provide information to either GAO or the Congress, we are concerned that public discussion of some of the details of our inquiry may go too

far toward disclosing security vulnerabilities and make it easier for individuals to compromise information that the Department has an obligation to safeguard. Accordingly, we respectfully request that the Subcommittee receive the details of our testimony in closed session. I can say, however, that we found patterns of neglect and inattention nationwide that parallel the circumstances that allowed the Kentucky incident to occur--deficiencies that we pointed out to Justice in 1988 and 1989.[1]

I might also mention, Mr. Chairman, that as of March 15, Justice had been unable to provide us with basic factual information such as the total number of employees in the U.S. Attorney's Offices nationwide. We received it just a few days ago. This is the kind of information that would allow some perspective on such issues as security training. In addition, the Executive Office was unable to tell us how much total surplus computer equipment from other U.S. Attorney's Offices contained sensitive information, and who the buyers were.

Our investigation leads to the unmistakable conclusion that at present, one simply cannot trust that sensitive data will be safely secured at the Department of Justice. The problems brought to light by the Kentucky incident and our investigation are systemic--

---

[1]Justice Automation: Security Risk Analyses and Plans for Project EAGLE Not Yet Prepared (GAO/IMTEC-89-65, Sept. 19, 1989).

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

and they require dedicated, Departmentwide, focused attention to bring about the changes that must be made, without delay.

Accordingly, because of the seriousness of this situation and the possibility of loss of life, we recommend that the Attorney General take the following actions immediately:

-- Identify all computer equipment surplused by Department components and determine whether it contained sensitive data.
-- Ensure that every Justice component that may have compromised sensitive data immediately prepare a damage assessment of the impact of the compromise on carrying out its mission and on the identity of such people as witnesses, confidential informants, and undercover agents.

Although the process is moving slowly, we acknowledge that Justice is hiring people to perform security compliance reviews throughout the agency and, therefore, we are making no recommendation on this specific issue at this time. We would caution Justice, however, that this hiring process needs to move forward with alacrity.

In addition, the Attorney General must move swiftly to establish effective computer security throughout the Department, in accordance with our previous recommendations. This should include

-- improving the leadership of the Justice Management Division and

the Security and Emergency Planning Staff by ensuring that the security staff (1) performs periodic audits and reviews of organizations within Justice that maintain sensitive data on ADP (automated data processing) systems, and (2) certifies that all such organizations are knowledgeable of Department security policies and procedures and have implemented adequate policies and procedures to ensure that violations of sensitive data do not occur in the future;

-- establishing mandatory computer security training, as required by the Computer Security Act of 1987, and monitoring Justice components' compliance with these requirements; and

-- reporting the compromising of sensitive data and various security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act, and discussing the actions that will be taken to correct these weaknesses.

Finally, we recommend that the Director of the Office of Management and Budget designate computer security at the Department of Justice as a high-risk area.