United States General Accounting Office

GAO

Testimony

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

For Release on Delivery
Expected at
2:00 p.m. EDT
Wednesday,
September 30, 1992

COMPUTER SECURITY

DEA's Handling of Sensitive Drug Enforcement and National Security Information Is Inadequate

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

Mr. Chairman and Members of the Subcommittee:

We are pleased to come before you once again to discuss computer security. And we regret that our message is not more positive. Once again a component of the Department of Justice is unable to adequately control its computer security operations. This time it's the Drug Enforcement Administration falling into this familiar pattern.

As you will recall, in 1990 we reported to you that Justice was not adequately protecting the highly sensitive computer systems of its litigating organizations and main data center.[1] In 1991 we testified before this Subcommittee about Justice's weak ADP security, the appalling story of excessed computer equipment that contained highly sensitive data, including grand jury material and information on confidential informants.[2] This time, it's the Drug Enforcement Administration's computer security. Our message today is strikingly similar to the messages we have delivered before: too little and much too late.

Our 15 months of investigation have revealed promises, beginning steps, and good intentions. But little has changed. DEA's handling of national security information, as we reported in February, was wholly inadequate.[3] Today, in releasing our latest report, we add to the story DEA's treatment of sensitive computer data.[4] The result is the same. Taken together, this situation places certain individuals at risk. And it can compromise the nation's effectiveness in combatting illegal drug distribution and use.

While DEA and the Department of Justice have begun to address discrete areas of concern, essential elements are lacking. An overarching structure. A strategy to guide continued action. Firm evidence of long-range commitment. Without these, Mr. Chairman, progress will remain sluggish, and the risks and dangers inherent in DEA's computer information operations will remain. The Attorney General must act with demonstrable seriousness in attacking this long-standing problem.

---

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

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

[3] Computer Security: DEA Is Not Adequately Protecting National Security Information (GAO/IMTEC-92-31, Feb. 19, 1992).

[4] Computer Security: DEA Is Not Adequately Protecting Sensitive Drug Enforcement Data (GAO/IMTEC-92-83, Sept. 22, 1992).

NATIONAL SECURITY INFORMATION AT RISK

As you know, in carrying out its critical work as the lead federal agency for enforcing drug laws, DEA relies heavily on computer and electronic communications systems to process highly sensitive drug enforcement and national security information.[5] This information can include the names of drug violators and informants, intelligence on drug trafficking organizations, and details of ongoing operations. Safeguarding such information from unauthorized access and disclosure is of paramount importance in protecting informants, maintaining public trust, and effectively combatting the illegal distribution and use of narcotics.

In response to our February report that DEA was not adequately protecting national security information processed on its computer systems, DEA officials said they were aware of no instances in which national security information entrusted to it had been compromised. They could not, however--and cannot---be sure that such has not occurred. Unauthorized access to and disclosure of this information could endanger lives and undermine ongoing law-enforcement investigations.

At DEA headquarters and the field locations we visited, the risk to DEA's national security data resulted from:

- Failure to comply with federal requirements for identifying computers that process national security information; in many cases DEA did not know what computers were processing classified data.
- Agency personnel who routinely processed classified information on computer equipment that was neither approved nor properly safeguarded for this use.
- Unusually lax physical security and a failure to adequately control access to areas in which classified data were being processed; non-DEA employees lacking clearances routinely worked unescorted in such areas, and computer disks and classified materials were often left unsecured.

Justice has found the same serious lapses in security at other DEA locations.

---

[5] Sensitive information is defined as any information that if lost, misused, or accessed or modified without authorization could adversely affect either 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)). National security information, also referred to as classified information, is official information or material that is owned by, produced by or for, or under the control of the U.S. government, and which requires protection against unauthorized disclosure in the interest of national security.

SENSITIVE DRUG-ENFORCEMENT DATA SIMILARLY VULNERABLE

As with national security information, DEA has serious computer security weaknesses that pose significant risks to the sensitive data the agency collects and uses. This disturbing situation exists because DEA has failed to implement an effective computer security program.

DEA Does Not Have an Effective Computer Security Program

DEA has not taken the basic steps necessary to protect computer systems that process sensitive drug-enforcement information. The Computer Security Act of 1987 requires that federal agencies identify computer systems that contain sensitive data and develop security plans for protecting these computer systems; it also requires that they establish mandatory computer security training so that all employees coming into contact with sensitive data and related systems fully understand their responsibilities and procedures for their protection. Further, as part of an effective computer security program, agencies must perform risk analyses and implement contingency plans for protecting access to and operation of sensitive computer systems.

Contrary to the mandate of the Computer Security Act and related federal policies, DEA has not put into place an effective computer security program that provides the necessary controls for safeguarding its sensitive computer systems and the data they contain. It has neither identified all systems processing sensitive data, nor completed security plans for them. Further, it remains vulnerable to service disruptions because it has not fully tested or implemented disaster contingency plans. And while training is underway, many personnel remain unaware of their security responsibilities. DEA has failed to comply with these basic requirements because computer security has not been an agency priority.

Specific Weaknesses: Lack of Security Controls, Unrestricted Access, Insufficient Recordkeeping, System Abuse

The lack of an effective computer security program at DEA has led to serious, fundamental weaknesses that pose significant risk to the integrity of its computer systems and the sensitive data they contain. For example, access--both to computer data and to the areas in which data disks and the computers themselves physically reside--is extremely lax. Moreover, fundamental protection measures such as passwords and audit trails are sloppily employed, if at all. In some instances, DEA employees used obvious passwords like "DEA," shared passwords, or--worse yet--left passwords taped to computer terminals. In addition, systems containing sensitive data were sometimes left turned on and accessible, even when no employees were present; computer disks containing sensitive data were left similarly unattended in open, unprotected areas.

Even more alarming is that contract cleaning and maintenance personnel--who lacked the necessary background security checks--were allowed to work unescorted in areas in which sensitive data were being handled in two DEA field offices. In one case, such individuals

were permitted to work alone in a room containing national security information as well as a computer used by DEA agents in ongoing investigations monitoring drug suspects' telephone calls. In violation of security rules, DEA agents had left sensitive case information, the system password, and instructions for accessing the system out in the open, next to the computer. In another case, we found a contract employee who had a criminal record that included an arrest for possession of a controlled substance. DEA was unaware of the individual's prior record until we pointed it out because the required investigative work, necessary to determine whether he or other contract employees posed a security risk, had never been completed.

Ineffective controls over computer equipment have also hampered attempts to improve security. Since 1988 DEA has been unable to develop an accurate inventory of the several thousand microcomputers that its employees use to process data; it therefore does not know whether any of these computers containing sensitive data have been lost or misused. And while agency policy prohibits the use of personally owned microcomputers for DEA work, this rule has not been adhered to.

I should interject, Mr. Chairman, that these problems were found at DEA's headquarters and in one or more of DEA's major divisions. In addition, the Department's Justice Management Division has found many of the same security weaknesses at seven DEA field locations.

Finally, we found instances in which agency employees and contract personnel, who had no need to know, were able to obtain and give sensitive computer data to individuals outside of DEA for personal reasons. For example, one DEA employee gave such information to a drug trafficker. This type of abuse could be controlled by (1) properly restricting computer access to those--and only those--with a demonstrated professional need for such information, and (2) reviewing available computer audit trail information to detect improper access to system data.

ACTIONS BY DEA, JUSTICE

Following our report on national security weaknesses, the DEA Administrator took immediate action to begin correcting the problems identified. For example, an agencywide directive was immediately issued prohibiting personnel from processing national security information on unprotected equipment. The Administrator also directed all field office heads to assign additional resources to addressing security needs. In addition, on-site reviews were initiated to ensure that procedures were in place for removing national security data from unprotected computer hard drives. Finally, with contractor support, DEA began conducting computer system risk analyses.

The Department of Justice, for its part, is taking a more active role in overseeing DEA compliance with computer security requirements. For example, it has implemented mandatory computer-security training throughout the Department and has performed computer-security compliance reviews at some of DEA's field offices.

The kinds of steps taken by both DEA and the Department of Justice are needed, and we applaud them. Yet a good deal more is required. DEA must take strong, aggressive action to put into place fundamental computer security safeguards over its many sensitive computer systems to protect them and their sensitive drug enforcement data from unauthorized use and potential compromise. In addition, continued vigilance on the part of Justice will be critical to realizing any long-term improvement.

AGGRESSIVE ACTION, CLOSE COORDINATION AND OVERSIGHT ESSENTIAL

To correct serious problems with DEA's handling of sensitive computer information, our report being released today recommends that the Attorney General direct the DEA Administrator to

- establish and implement an effective agencywide computer security program that complies with all federal and departmental directives,
- strengthen DEA's monitoring and oversight of computer security,
- ensure that weaknesses identified are corrected and that similar weaknesses do not exist elsewhere, and
- report computer security weaknesses at DEA as a material internal control weakness under the Federal Managers' Financial Integrity Act.

We also recommend that the Attorney General direct the Justice Management Division to work closely with DEA to ensure that these recommendations are carried out and that DEA complies with all federal and departmental computer security requirements.

- - - - -

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.