United States General Accounting Office

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

[redacted]

139646

GAO

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

Information Management and
Technology Division

B-249689

September 22, 1992

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

Dear Mr. Chairman:

In response to your request, on August 25, 1992, we provided your office with a Limited Official Use report discussing the results of our review of DEA's compliance with federal computer security laws and regulations and the Justice Department's oversight of DEA's compliance with these requirements. It included recommendations to the Attorney General and the DEA Administrator aimed at improving the effectiveness of DEA's computer security program and correcting fundamental computer security weaknesses that exist. The report supplemented earlier work, Computer Security: DEA Is Not Adequately Protecting National Security Information (GAO/IMTEC-92-31, Feb. 19, 1992).

As agreed with DEA and the Justice Department, in this public version of the report we removed references to specific DEA offices or office locations. This avoids making it easier for individuals to compromise sensitive drug enforcement data that the agency has an obligation to protect.

Unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of this letter. At that time we will send copies to the Department of Justice, DEA, and the Office of National Drug Control Policy. We will also send copies to other interested parties upon request.

This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who can be reached at (202) 512-6418. Other major contributors are listed in the appendix.

Sincerely yours,

Ralph V. Carlone

Ralph V. Carlone
Assistant Comptroller General

Executive Summary

Purpose

The Drug Enforcement Administration (DEA) is the lead federal agency for enforcing drug laws and investigating the illegal distribution and sale of narcotics. In carrying out this mission, DEA uses computer systems to process a variety of highly sensitive information. Unauthorized disclosure of this information could disrupt DEA operations and adversely affect the nation's war on drugs.

At the request of the Chairman of the Government Information, Justice, and Agriculture Subcommittee, House Committee on Government Operations, GAO assessed the adequacy of DEA's computer security. Specifically, GAO evaluated (1) the extent to which the agency has complied with the Computer Security Act of 1987 and federal computer security requirements designed to protect sensitive computer information, and (2) Department of Justice oversight of DEA compliance with federal and departmental requirements. GAO's work focused on DEA's compliance with computer security requirements for sensitive information only. GAO's work on DEA computer security weaknesses involving national security information is discussed in its February 1992 report.[1]

Background

To carry out its mission of enforcing federal drug laws, DEA relies on computer and electronic communications systems to collect, process, store, and transmit a variety of highly sensitive information. This information includes investigative data such as the names of drug violators and informants, intelligence on drug trafficking organizations, and details on ongoing operations to counter illegal drug smuggling. If this information is not protected from unauthorized access and disclosure, individuals could be harmed, public trust eroded, and the success of the nation's war on drugs jeopardized. DEA must ensure, therefore, that its computer systems are subject to stringent security provisions and oversight.

The Computer Security Act of 1987 (P.L. 100-235) requires federal agencies to identify and develop security plans for protecting computer systems that they designate as containing sensitive information and to establish mandatory computer security training to make employees aware of their specific responsibilities. Federal policies further direct agencies to protect access to and operation of sensitive computer systems by conducting risk analyses and implementing contingency plans, critical first steps for

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

ensuring the establishment of necessary security safeguards and continuity of data processing if normal operations are interrupted.

Results in Brief

DEA is not adequately protecting sensitive information processed on its computer systems. It has not fully complied with the Computer Security Act or with basic federal and departmental computer security requirements. As a result, DEA has serious and fundamental computer security weaknesses that collectively pose a significant risk to the integrity of DEA's computer systems and the sensitive data they contain. This disturbing situation exists because DEA has failed to implement an effective agencywide computer security program or to establish adequate computer security controls. In response to the serious deficiencies GAO found, DEA has begun to take some corrective action.

In addition, while the Department of Justice is improving its oversight of computer security, it needs to work more closely with DEA to ensure that the agency complies with all federal and departmental computer security requirements.

Principal Findings

DEA Does Not Have an Effective Computer Security Program

DEA does not have an effective computer security program to provide necessary security controls for safeguarding its sensitive computer systems. Contrary to the Computer Security Act of 1987, DEA has neither identified all of its computer systems processing sensitive data nor completed security plans for these systems. Moreover, DEA has not followed federal guidance and taken fundamental steps to adequately protect the data contained in these computer systems. For example, at the beginning of our review, the agency had not completed risk analyses to identify and minimize security threats for any of its sensitive computer systems. Furthermore, DEA's computer operations are highly vulnerable to disasters and prolonged service disruptions because it has not fully tested and implemented contingency plans for agency data processing facilities and systems.

In addition, DEA management has failed to effectively monitor and enforce computer security. Agency personnel are often unaware of their computer security responsibilities because DEA's computer security awareness

training has not been effective and its computer security guidance has been either inadequate or poorly communicated. DEA has begun to address this problem by developing and distributing additional security procedures for protecting the processing and storing of some of its sensitive computer data.

Serious Computer Security Weaknesses Exist

DEA is not adequately safeguarding its sensitive computer data. DEA personnel at headquarters and two of the agency's field divisions routinely process sensitive data on microcomputers that lack fundamental security controls, such as password protection and audit trails for preventing and detecting unauthorized access. In cases where password protection was used, DEA personnel shared passwords, and in a few cases, left them taped to computer terminals or used passwords that could easily be compromised. Moreover, GAO found many instances in which DEA personnel left computers containing sensitive information unattended and turned on, thus providing easy access to the data. GAO also found cases in which floppy diskettes and other documents containing sensitive drug information were left unattended in open, unprotected areas.

The seriousness of these computer security weaknesses is compounded by DEA's ineffective controls over access to areas where computers process sensitive data. For example, at the two division offices GAO visited, contract maintenance personnel who had incomplete or unfavorable background investigations were allowed to work unescorted in areas where sensitive computers were used. In one instance, security personnel were unaware that an individual, employed by a contractor and working unescorted in the facility, had a criminal record, including an arrest for possession of a controlled substance. In another case, a computer system used by DEA agents in ongoing investigations monitoring drug suspects' telephone calls was left totally unprotected. In this case, the computer was in an open room where everyone, including non-DEA employees, such as unescorted janitorial and maintenance personnel, routinely worked. Moreover, DEA agents left the system password and instructions for accessing the system out in the open next to the computer.

DEA also has longstanding weaknesses in its controls over computer equipment. Since 1988 DEA has not been able to develop an accurate inventory of the several thousand microcomputers that its employees use to process DEA data. As a result, the agency has no way of knowing whether any of its computers containing sensitive information have been lost or misused. For example, in one division office, administrative

personnel were unable to account for all their computer equipment because of poor record-keeping practices. Sensitive data are also left exposed to unauthorized disclosure because of lax computer maintenance practices and failure to comply with agency policy prohibiting the use of personally owned microcomputers.

While GAO's review involved DEA headquarters offices and offices of two major divisions, the department's Justice Management Division has found many of the same security weaknesses at seven DEA field locations.

In addition, GAO's review of DEA Office of Professional Responsibility records also found instances in which sensitive computer information has been improperly used or disclosed to unauthorized individuals outside the agency. For example, GAO found instances in which DEA administrative personnel and non-DEA contractor personnel without a need to know obtained sensitive data about their friends and acquaintances from DEA computer systems. Such access is possible because DEA lacks controls to prevent individuals who have access to DEA computers from obtaining data outside their areas of responsibility.

Justice Oversight Has Improved

The Department of Justice is taking a more active role in its oversight of DEA's compliance with computer security requirements. For example, Justice has implemented mandatory computer security training throughout the department and has begun to perform compliance reviews at DEA field offices. Given the weaknesses GAO found, however, the department's Justice Management Division needs to work more closely with DEA to ensure that the agency complies with all federal and departmental computer security requirements. This includes ensuring that DEA conducts complete risk analyses and provides Justice with accurate annual computer security status reports on the adequacy of DEA's computer security safeguards.

Recommendations

GAO recommends that the Attorney General direct the Administrator of the Drug Enforcement Administration to (1) establish and implement an agencywide computer security program that complies with all federal and departmental computer security directives, (2) strengthen DEA's monitoring and oversight of computer security, (3) ensure that the computer security weaknesses identified in this report are corrected and that similar weaknesses do not exist elsewhere, and (4) report the

computer security deficiencies at DEA as a material internal control weakness under the Federal Managers' Financial Integrity Act.

In addition, GAO recommends that the Attorney General direct the Justice Management Division to work closely with DEA to ensure that the agency implements GAO's recommendations and that DEA complies with all federal and departmental computer security requirements.

Agency Comments

As requested, GAO did not provide a draft of this report to Justice and DEA for review and comment. However, GAO discussed the report's contents with Justice and DEA officials, who generally agreed with the facts presented. We have incorporated their views in the report as appropriate.

Contents

Abbreviations

ADP	automated data processing
DEA	Drug Enforcement Administration
FIRMR	Federal Information Resources Management Regulation
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
NADDIS	Narcotics and Dangerous Drug Information System
OMB	Office of Management and Budget
OPR	Office of Professional Responsibility

Introduction

The Drug Enforcement Administration (DEA) uses computer systems to process a variety of highly sensitive information used in the enforcement of federal drug laws. DEA computer systems contain descriptive information on known or suspected drug violators, informants, and undercover law enforcement officials, as well as national security information such as foreign drug intelligence. If DEA fails to protect this information from unauthorized access and disclosure, lives could be endangered or lost and investigations that impact successful drug enforcement could be severely undermined.

The Computer Security Act of 1987 (P.L. 100-235) and other applicable federal laws and regulations require government agencies to adequately protect the sensitive information that they process on computers.[1] Specifically, the Computer Security Act requires federal agencies to identify and develop security plans for computer systems that they designate as containing sensitive information and establish mandatory computer security training to make employees aware of their specific responsibilities. In addition, federal policies direct agencies to protect access to and operation of sensitive computer systems by conducting risk analyses and implementing contingency plans,[2] critical first steps for ensuring the establishment of necessary security safeguards and continuity of data processing. To fulfill these requirements, Department of Justice policy requires component agencies, including DEA, to establish and implement computer security programs to provide the necessary safeguards for protecting access to and operation of computer systems that contain sensitive information.

Computers Processing Sensitive Information Are Critical to DEA's Mission

DEA enforces laws and regulations relating to the use and distribution of legal and illegal drugs. The agency accomplishes its mission through a centralized organization consisting of over 7,000 employees and agents, who work at headquarters and domestic offices as well as foreign offices located worldwide. In conducting drug investigations, DEA agents and investigators collect information by interviewing witnesses, subpoenaing documents, conducting surveillance, working undercover, recruiting confidential informants, making arrests and executing search warrants, and performing other law enforcement duties.

[1]The Computer Security Act defines sensitive information 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)).

[2]Office of Management and Budget (OMB) Circular No. A-130, App. III., Management of Federal Information Resources, (Dec. 12, 1985).

DEA operates computer systems to process and store the sensitive investigative information it collects. An important part of DEA's automated data processing capability is its Office Automation system. The system, which is a microcomputer-based network of workstation clusters and is currently operated in most domestic DEA locations, provides the agency with a standardized network of computers for data processing and network data exchanges between DEA offices. The workstation clusters are configured around master workstations that provide local data processing and communications with other workstations on the network. DEA is currently planning a multimillion dollar acquisition to improve and expand its office automation capabilities.

DEA uses the Office Automation system to process sensitive information and, through communication software, to access other sensitive databases, such as DEA's Narcotics and Dangerous Drugs Information System (NADDIS). NADDIS and other large database systems are stored on mainframe computers at Justice's main data center in Rockville, Maryland, and are linked to Office Automation workstations and other computers in DEA offices through the agency's Network Control Center. In addition, DEA agents and other personnel throughout the agency use about 3,000 microcomputers to collect, process, and store sensitive drug enforcement data.

DEA Actions to Correct Weaknesses Involving Computers That Process National Security Information

In February 1992, we provided the Chairman of the Government Information, Justice, and Agriculture Subcommittee, House Committee on Government Operations, with a report documenting serious weaknesses involving the processing of national security information on DEA computer systems.[3] Our review found that, contrary to Justice policy, DEA had failed to identify its computers that process national security information. Moreover, we found that agency personnel were improperly using unapproved and unprotected computer equipment to process national security information and that this equipment was used in areas where access was not adequately controlled.

In response to our report, DEA took immediate action to begin correcting the weaknesses we found. For example, DEA issued an agencywide directive prohibiting personnel from processing national security information on computer equipment that was not properly protected. In addition, the DEA Administrator directed all field office heads to assign

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

additional resources to address security needs. DEA's Office of Information Systems also began conducting on-site reviews to ensure that procedures were in place for removing national security information left residing on unprotected computer fixed-disks. This office also completed negotiations with a contractor to begin work on computer system risk analyses.

Objectives, Scope, and Methodology

At the request of the Chairman of the Government Information, Justice, and Agriculture Subcommittee, House Committee on Government Operations, we reviewed the adequacy of DEA's computer security. Specifically, we evaluated (1) the extent to which the agency has complied with the Computer Security Act and other federal computer security requirements for protecting sensitive computer information, including risks associated with any deficiencies; and (2) Department of Justice oversight of DEA compliance with federal and departmental requirements.

To assess DEA's efforts to comply with the Computer Security Act and other federal computer security laws and regulations, we compared these requirements with DEA's policies and procedures for safeguarding sensitive information. We also examined internal DEA reports documenting security inspections and surveys and reviewed closed case files summarizing DEA's internal investigations of employees who allegedly disclosed sensitive computer information to unauthorized individuals.

In addition, to assess how computer security practices are carried out, we interviewed DEA personnel responsible for computer security at DEA headquarters and at the offices of two of the agency's field divisions, hereafter referred to as Division A and Division B.[4] We selected these locations because of the high number of drug investigations they conduct and their extensive use of computers in processing investigative data. At these locations, we observed and evaluated computer security practices followed by agency personnel in protecting sensitive information processed on DEA computers. We also visited DEA's Network Control Center to review the agency's emergency response, back-up, and recovery capabilities for computer data transmissions.

To assess Department of Justice oversight activities, we met with Justice computer security personnel and reviewed Justice computer security policies. We also examined compliance review reports prepared by the

[4]As agreed with DEA and the Department of Justice, in this public version of the report we removed references to specific DEA offices or office locations. This avoids making it easier for individuals to compromise sensitive drug enforcement information that the agency has an obligation to protect.

Justice Management Division documenting its assessments of computer security at various DEA field locations.

Although our review focused on major elements of DEA's overall computer security program, it did not assess the security of DEA's mainframe computer systems at the Justice Data Center. We reviewed the adequacy of security safeguards at Justice's main data center as part of an earlier review.[5] Our work was performed between June 1991 and August 1992, in accordance with generally accepted government auditing standards.

As requested, we did not obtain written agency comments on this report. However, we discussed the report's contents with Justice Department and DEA officials, including the Assistant Attorney General for Administration and DEA's Assistant Administrator, Planning and Inspection Division. We have incorporated their views where appropriate.

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

DEA Does Not Have an Effective Computer Security Program

The Computer Security Act requires federal agencies to identify computer systems that process sensitive information, develop security plans for these systems, and establish mandatory computer security training. Federal policies further require agencies to establish overall computer security programs for protecting access to and operation of sensitive computer systems by conducting risk analyses and by implementing contingency plans.[1]

However, DEA has not fully complied with all these requirements because computer security has not been a priority of the agency. Moreover, while the Department of Justice has begun to monitor DEA compliance with computer security requirements, more effective oversight is needed. Collectively, these limitations have led to serious breakdowns in computer security, as discussed in chapter 3.

Fundamental Computer Security Requirements Have Not Been Met

DEA has not taken the fundamental steps necessary to ensure the protection of sensitive data processed on its computer systems. Specifically, DEA has not identified all of its computer systems used to process sensitive information, nor has the agency completed the required security plans. Although DEA is conducting mandatory computer security awareness training, we found that agency personnel were still unaware of their computer security responsibilities because this training was limited and agency computer security guidance has been inadequate or poorly communicated. In addition, DEA has not completed required risk analyses for all of its sensitive computer systems to identify vulnerabilities and has not fully tested and implemented a contingency plan for ensuring continued processing throughout DEA should computer service disruptions occur.

Sensitive Computer Systems Not Identified and Security Plans Not Complete

The Computer Security Act requires agencies to identify all computer systems that contain sensitive information and prepare security plans for each identified system. The act defines a computer system as,

"...any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information..."

[1]OMB Circular No. A130, App. III, Management of Federal Information Resources, Dec. 12, 1985; Federal Information Resources Management Regulation (FIRMR) (41 C.F.R. part 201-7); and U.S. Department of Justice, Automated Information Systems Security (DOJ 2640.2B), Nov. 16, 1988.

In January 1989, in response to the Computer Security Act, Justice reported that DEA operated seven major computer systems that contained sensitive information. In November 1990, Justice asked its components to provide it with updated lists of sensitive computer systems. In November 1991, after we began our review, DEA provided Justice with an updated list that identified 10 major sensitive computer systems and subsystems.

However, DEA's updated list does not identify some of its microcomputer-based systems, despite regular use of these systems to store, manipulate, and manage various kinds of sensitive data. For example, the list failed to include the Target Analysis and Reporting System, which is currently used by DEA agents in foreign countries to store informant information and collect highly sensitive investigative data on suspected drug traffickers and their illegal activities. Also omitted was a computer system that collects telephone data on suspected drug traffickers. According to DEA agents, unauthorized disclosure of information contained in this system could jeopardize ongoing investigations.

DEA's updated list also excluded the Security Investigative System. According to Justice documentation, DEA had previously reported this as a sensitive system under the Computer Security Act because it contains background investigations and clearance information on DEA agents, personnel, and contractors. Since the system was recently converted from a mainframe application to a microcomputer-based system, DEA's Assistant Administrator for Operational Support stated in a memorandum to the Department of Justice that the system no longer needed to be reported. However, the Act clearly requires agencies to identify and prepare security plans for all computer systems that contain sensitive data; consequently, all such microcomputer systems need to be identified. Sufficient information was not available for us to determine how many other DEA microcomputer systems being used to process sensitive data have not been identified and properly reported by the agency.

DEA has also not completed and implemented security plans for its sensitive systems, and therefore is not in full compliance with the Computer Security Act and other federal guidelines.[2] While draft security plans have been prepared for some computer systems, DEA cannot finalize and implement them because it has not completed other computer

[2]OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, July 9, 1990.

developing comprehensive security plans. Moreover, we found that DEA's draft security plans lacked important information about the computer systems they discussed. For example, the draft plan for the NADDIS system did not clearly identify all relevant subsystems or the functionality and associated controls for the subsystems.

Risk Analysis Requirement Not Met

Risk analyses are an important part of a computer security program and a fundamental step for protecting computer systems and the data they contain. Office of Management and Budget Circular A-130 requires federal agencies to perform a risk analysis at least every 5 years to ensure that appropriate, cost-effective safeguards are incorporated into existing and new computer installations including networks.[3] Specifically, risk analyses help agencies identify computer security threats and establish needed safeguards for countering these threats. Nevertheless, at the beginning of our review, DEA had not completed risk analyses for any of its sensitive computer systems. DEA officials could not explain why the agency had not complied with this fundamental requirement.

Despite its use of sensitive computer systems, such as NADDIS, which has been in operation for 20 years, DEA only recently began to perform risk analyses. Moreover, its work to address this fundamental computer security requirement has been limited so far and remains incomplete. In the last 2 years, DEA contracted with a private company to perform risk analyses of two DEA sensitive systems—NADDIS and the Office Automation system. In 1991 the contractor provided DEA with draft reports of its work on both these systems. These reports noted serious security weaknesses in both systems. For example, the Office Automation system lacked fundamental system access controls, such as software that automatically removes data from computer workstation screens if a workstation is left unattended. The draft NADDIS study cited numerous computer security weaknesses, including inadequate controls for preventing unauthorized use of workstations that access sensitive NADDIS data. However, DEA officials told us they took only limited action to address vulnerabilities pointed out in these studies because DEA's Office of Information Systems rejected the contractor's work based on disagreements with the contractor's risk analysis methodology. Nevertheless, many of these same security weaknesses were found during our review and in security compliance reviews recently conducted by Justice (see ch. 3).

[3]OMB Circular No. A-130, App. III, Dec. 12, 1985.

In June 1991, DEA again contracted to perform risk analyses of NADDIS and other major DEA sensitive computer systems. In August 1992, DEA officials advised us that the contractor completed its first risk analysis in April 1992, and that the contractor would complete the remaining risk analyses by the first quarter of 1993. Like the earlier studies, the risk analyses completed to date have identified extensive and widespread computer security weaknesses, including many of the same weaknesses we found during our review. For example, the contractor studies reported that DEA's computer security awareness training was inadequate, access to sensitive computers and computer material was not controlled, and security policies and procedures were deficient or not being followed.

Moreover, the risk analyses being performed by the current contractor may not identify all existing computer system vulnerabilities because the contractor's work is limited in scope and does not address all departmental requirements. For example, at the time of our review the contractor told us that DEA was not requiring the assessment of vulnerabilities and risks at field offices where many of these sensitive computer systems are either remotely accessed or used. Moreover, the contractor acknowledged that its work on NADDIS and other major DEA sensitive computer systems does not include assessing the adequacy of controls for safeguarding sensitive data transmitted over network communication lines.

Contingency Plans Not Fully Tested or Implemented

DEA has not fully tested and implemented contingency plans for any of its data processing facilities and systems to ensure adequate emergency response, backup, and recovery procedures as required by departmental and other federal requirements. As a result, in the event of an emergency, DEA is at high risk of experiencing a catastrophic loss that would cripple the agency and its ability to perform basic computer processing necessary for carrying out its drug enforcement mission. For example, DEA lacks adequate backup and recovery measures to ensure the continuation of critical services provided by the agency's Network Control Center. The Network Control Center functions as DEA's primary nerve center and single point through which all of the agency's sensitive and national security data transmissions are handled. If services at the center are destroyed or disrupted for a prolonged period, DEA would lose the computer data processing it needs to support its ongoing operations. Despite this, the agency has not established an alternative site capable of taking over these vital functions in emergency situations. In August 1992, DEA's Deputy Assistant Administrator for Information Systems told us that DEA and

Justice had agreed on a proposed alternative site for the Network Control Center.

Citing DEA's lack of emergency response, backup, and recovery procedures for its data processing facilities and systems, a July 1989 Justice internal audit recommended that DEA take immediate action to develop and implement contingency plans to ensure continued processing of the agency's mission critical systems.[4] Yet, as of August 1992, DEA was still operating its computer systems and data communications without clearly established emergency response, backup, and recovery measures in place. Although agency management approved a draft continuity of operations plan providing for the continued processing of DEA's most critical systems in August 1991, DEA has still not fully tested the plan or addressed the backup and recovery needs for all DEA facilities and computer systems.

DEA Computer Security Awareness Training and Guidance Has Not Been Adequate

DEA's Office of Security Programs is responsible for implementing a computer security awareness training program for DEA employees and for issuing guidance to familiarize agency personnel with their individual computer security responsibilities. Although the Office of Security Programs has provided DEA employees with computer security awareness training, its effectiveness is questionable. In the case of a Division A district office, for example, this training consisted mainly of having employees read several memos on computer security and sign an agreement that they had received security training. Moreover, Justice compliance reviews conducted between November and December 1991 at three DEA field offices also found DEA's computer security education has not been adequate to familiarize all personnel with their individual security responsibilities for protecting DEA information processed on computers.

Inadequate or poorly communicated computer security guidance further exacerbates this problem. For example, DEA has no comprehensive policy addressing the appropriate use and protection of microcomputer equipment, despite the agency's extensive use of about 3,000 microcomputers. Moreover, although the Office of Security Programs has prepared computer security policy bulletins, the bulletins are not always distributed to all DEA offices. For example, in July 1991 the security officer responsible for computer security at one of DEA's larger field divisions told us she did not have any copies of departmental security orders or policy

[4]U.S. Department of Justice, Office of Inspector General, The Drug Enforcement Administration's Automatic Data Processing General Controls, A89-4, July 1989, pp. ii, 31-32.

memoranda. A Justice compliance review conducted 5 months later found that the security officer still did not have any security orders or policy memoranda, even though at least seven such policy memorandums were issued during this time. In addition, an agency security official told us that computer security bulletins had not been distributed to DEA headquarters offices. In response to our work, in April 1992 DEA's Office of Security Programs redistributed security memorandums to DEA field office assistant special agents-in-charge and security officers.

Moreover, DEA's computer security bulletins were sometimes unclear and confusing. For example, while one security bulletin explicitly prohibited personnel from storing any sensitive information on computer fixed disks, a contradictory bulletin issued one week later by the same office directed DEA personnel not to release fixed disks containing sensitive information to non-DEA personnel. DEA's own internal assessment of NADDIS security in April 1991 concluded that DEA computer security policies were obsolete, fragmented, and in need of revision. In response to our earlier report and current review, DEA officials told us in August 1992 that the agency had developed and distributed additional security guidance to clarify procedures for processing and storing sensitive information on Office Automation computers. If correctly implemented by all personnel, these revised procedures should improve the security safeguards over data processed on DEA Office Automation computers.

DEA Is Not Effectively Monitoring Computer Security

The security programs manager of the Office of Security Programs—the automated data processing security officer for DEA—has agencywide responsibility for computer security. According to the security programs manager, security officers in each DEA office and field unit have been assigned responsibility for monitoring and enforcing computer security. In addition, the security programs manager told us that staff from DEA's Office of Security Programs conduct periodic surveys to assess compliance with general security requirements at agency offices and field locations. However, our review found that security officers and the security staff are not effectively monitoring or enforcing computer security.

Security Personnel Do Not Monitor and Enforce Computer Security

At both divisions we visited the designated security officers were not monitoring computer security and were not taking adequate steps to safeguard sensitive computers and data. For example, at Division B the security officer told us he did not monitor computers used by division staff

to process sensitive data because no inventory of these systems had ever been compiled. In fact, during our tour of the facility, the security officer told us he did not know which computers were used to process sensitive data. In addition, both divisions' security officers were not performing basic security tasks, such as monitoring access to areas where sensitive computers and data were located. At Division A, for example, the security officer did not review card-key access logs to determine if attempts to gain entry to areas where sensitive information was collected, processed, and stored were made after normal business hours. Moreover, the security officer kept no records documenting the results of security checks on janitorial and maintenance personnel who entered and worked in the facility. In fact, until we pointed it out, the Division A security officer was not aware that a non-DEA employee (janitor) possessed and used a card-key for accessing division offices at any time. At Division B, when we observed unescorted janitors working before regular business hours, the security officer could not tell us how these individuals had entered the facility because he did not track contractor access to the facility.

The security officers told us they did not monitor computer security because they were generally unaware of their computer security responsibilities, had too many other duties, and had little or no training and computer-related experience. According to the security officers at both division locations, they had not read and were not familiar with basic departmental and DEA computer security requirements because computer security is a low priority and other duties are considered more important. For example, the designated security officer role for Division A was assigned to the Assistant Administrative Officer, who also fulfilled many other administrative responsibilities. Further, both the Division A and Division B security officers considered themselves to be computer illiterate and admitted that they had received no computer or computer security training prior to their appointment as security officers.

DEA Security Surveys Are Not Effective in Identifying Computer Security Weaknesses

According to the security programs manager, the Office of Security Programs conducts security surveys to review the adequacy of basic security measures at DEA field locations. However, the effectiveness of these surveys in identifying and correcting computer security weaknesses is highly questionable. First, according to a DEA official on the security survey teams, only minimal time and attention are devoted to assessing computer security. Second, the reviews are only performed about every 3 years. Third, and most important, the DEA official responsible for performing these reviews told us that he and his staff have limited

computer experience and little knowledge of computer security. In fact, our random review of 11 of the more than 50 security surveys conducted since January 1990 showed that the surveys identified few if any computer security weaknesses. For example, DEA's May 1991 survey of Division A reported no computer security weaknesses. This was in stark contrast to the extensive weaknesses that we found at this location 2 months later (see ch. 3).

DEA Action to Improve Computer Security Monitoring Is Insufficient

In January 1992, after we briefed DEA on the national security weaknesses we found during our review,[5] DEA's Administrator directed all division special agents-in-charge, headquarters office heads, country attachés, and laboratory directors to designate an assistant special agent-in-charge or other appropriate individual to serve as security manager for each division and foreign and domestic office. The newly appointed division security managers were directed to work with the designated security officers to focus more attention on security and computer security related matters.

While such action is a positive step and clearly demonstrates DEA's commitment to improving agency computer security oversight, it will not totally resolve the problems we identified. Specifically, DEA has not developed written guidance detailing computer security responsibilities for the newly appointed security managers and the existing security officers. Moreover, DEA's security programs manager told us that the agency has no immediate plans to provide security managers with additional training for carrying out their computer security responsibilities. It is also unclear how DEA's action to appoint security managers will enable security officers, who are already overburdened with other assigned duties, to better carry out their computer security responsibilities.

Improved Justice Oversight Has Not Ensured DEA's Computer Security Compliance

The Department of Justice has responsibility for oversight of computer security in all Justice component agencies, including DEA. Specifically, the department's Justice Management Division is responsible for establishing computer security policies and for enforcing compliance with these and other federal policies. However, in a prior review we found that the Justice Management Division had not been effectively carrying out its oversight responsibilities.[6] In our report, we recommended that Justice take the

[5]The national security weaknesses we found are discussed in our report Computer Security: DEA Is Not Adequately Protecting National Security Information (GAO/IMTEC-92-31, Feb. 19, 1992).

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

necessary steps to ensure the adequacy of computer security safeguards in department component organizations. The Justice Management Division has since begun to implement our recommendations and has taken some action to ensure DEA's compliance with federal and departmental computer security requirements. For example, the Justice Management Division implemented mandatory computer security awareness training; as of January 1992, Justice reported that 95 percent of all departmental employees had received this training. As noted earlier, however, DEA's computer security awareness training has not been adequate.

In addition, last year the Justice Management Division established compliance review teams and began conducting reviews at DEA to identify and correct computer security weaknesses. As of June 1992, the division had completed security compliance reviews at 7 of the more than 200 DEA offices. As discussed in chapter 3, these reviews pointed out many serious computer security weaknesses, such as the improper processing of national security information on unprotected computer equipment. The Justice Management Division is now working with DEA to correct weaknesses that were identified at each of the seven locations.

While we support this effort, the Justice Management Division also needs to work more closely with DEA to ensure that it complies with all other departmental computer security requirements. For example, as discussed earlier, DEA has not completed required system risk analyses that meet minimum departmental requirements.

A departmental directive also requires each Justice component to annually report on the status of computer security to the department's security officer.[7] However, we found that DEA's 1990 annual security status report was inaccurate. In the report, submitted to Justice in November 1991, DEA incorrectly stated that it did not process national security information on any of its computer systems. Consequently, the report provided no information on the adequacy of DEA's security safeguards for protecting this type of information. The Justice Management Division should have known that DEA's report was inaccurate, especially since a division security compliance review pointed out in August 1991 that DEA was not adequately safeguarding the national security information it routinely processes on computers. Nevertheless, the Justice Management Division did not question DEA about the accuracy of its security status report because, according to a Special Assistant to Justice's Security Officer, division staff do not check the accuracy of security status reports

[7]Department of Justice 2640.2B, Nov. 16, 1988.

submitted by departmental components. In fact, DEA took no agencywide action to correct weaknesses in processing and storing national security information until we advised it of these problems in December 1991.

Serious and Fundamental Computer Security Weaknesses Exist

DEA's failure to establish an effective computer security program has led to many serious and fundamental security weaknesses. These weaknesses include a lack of safeguards over sensitive computers and data, inadequate controls over access to sensitive areas, and no accountability over or control of sensitive computer equipment. While our review included only DEA headquarters offices and offices of two major field divisions, the department's Justice Management Division recently found similar types of computer security weaknesses at seven DEA field locations.

In addition, DEA's Office of Professional Responsibility has investigated instances in which DEA employees, as well as non-DEA personnel such as contractors, allegedly disclosed sensitive computer information to unauthorized individuals. Our review of these investigations showed that individuals who were authorized access to DEA computers had obtained and misused sensitive computer information they did not have a need to know. These instances occurred because DEA has not instituted controls that prevent individuals, who have access to DEA computers, from obtaining data outside their areas of responsibility.

Sensitive Computer Data Not Adequately Safeguarded

DEA is not adequately safeguarding its sensitive computer data. DEA personnel routinely use computers that lack fundamental security safeguards to process and store sensitive data. These computers are also frequently left signed on[1] and unattended, thus providing easy access to the information they contain. Further, we observed numerous instances in which unprotected floppy diskettes and computer-generated documents were left unattended in unsecured areas. Collectively, these weaknesses, summarized in table 3.1, substantially increase the risks of unauthorized disclosure of sensitive information.

[1]A computer operational state allowing a user to access data files and retrieve information.

Table 3.1: Weaknesses in Controlling Access to Sensitive Computer Data at DEA Headquarters and Divisions

	DEA Headquarters	Division A	Division B
Access to Sensitive Computer Data Not Controlled			
Microcomputers lack passwords for restricting access to sensitive data	X	X	X
Microcomputers lack audit trails for detecting unauthorized access	X	X	X
Users sharing system passwords	X	X	X
System passwords left taped to computers	X	X	X
Easily compromised passwords used by personnel[a]	X	X	
Unattended computers left signed on	X	X	X
Sensitive Computer Materials and Documents Left Unprotected			
Computer-generated materials left unattended and unsecured		X	X
Unsecured facsimile equipment used to transmit sensitive data		X	
Documents left unattended and unsecured	X	X	X
Safes left open and unattended	X	X	

[a] Easily compromised passwords include common names (e.g., a person's first name) or sets of numbers (e.g., a person's street address) that are obvious to others.

Access to Sensitive Computer Data Not Controlled

We found that, contrary to federal guidelines and departmental policy, DEA personnel routinely processed sensitive drug investigative data on computers that lacked fundamental security safeguards. For example, in many cases microcomputers used by DEA personnel to process and store sensitive data had no password protection and audit trails for preventing and detecting unauthorized access. DEA has been testing various microcomputer security software products that, according to agency officials, will provide basic security safeguards such as passwords and audit trails. However, as of August 1992, DEA had not begun to install these products on its several thousand microcomputer systems.

DEA is also not taking basic security steps to protect access to computers containing sensitive information. For example, we noted many instances

in which Office Automation system passwords were not adequately safeguarded by DEA personnel. Instead DEA personnel shared passwords, and in a few cases, left them taped to computer terminals or used passwords such as "DEA" that could easily be identified. In many other cases, DEA employees left both Office Automation workstations and microcomputers signed on and unattended, allowing unauthorized individuals direct access to the data they contained.

Sensitive Computer Materials and Documents Left Unprotected

We also found security weaknesses in the methods DEA personnel use to handle computer-generated materials and documents containing sensitive information. For example, contrary to departmental and agency policy, at DEA headquarters offices and the two division offices, floppy diskettes and other documents containing sensitive investigative reports were routinely left unattended in open and unprotected areas. These areas were within easy access of everyone, including non-DEA personnel who were working in the facilities.

At a district office of Division A, we observed an unsecured facsimile machine, located in an unprotected area, with what we were told was a sensitive document lying unattended in the machine tray. The document, transmitted from a foreign country, disclosed the name and social security number of a DEA agent working in the country, as well as the name of the ongoing DEA operation in which the agent was involved. A Division A Regional Agent-in-Charge acknowledged that the information should have been transmitted using a secure facsimile machine because compromising this information could potentially jeopardize the operation and endanger the lives of the DEA agents.

Nevertheless, we were told that the office did not have secure facsimile equipment to receive and transmit sensitive data. We believe this is a serious security breach, especially since sensitive information could be exposed to unauthorized individuals if, by incorrectly dialing the facsimile telephone number, information is transmitted to a wrong location.

Inadequate Controls Over Access to Sensitive Areas Further Jeopardizes Security

Weaknesses in DEA's procedures for controlling access to areas where computers process and store sensitive data compound the serious computer security problems discussed above. Contrary to Justice policy, DEA was not adequately investigating the backgrounds of nonagency personnel who had unescorted access to sensitive areas. DEA also did not have adequate physical safeguards in place to control access to areas

where computers process sensitive information. The weaknesses we found are summarized in table 3.2.

Table 3.2: Weaknesses in Controlling Access to Sensitive Areas at DEA Headquarters and Divisions

	DEA Headquarters	Division A	Division B
Individuals without background investigations or security clearances working unescorted in sensitive areas		X	X
Doors to sensitive areas left open	X	X	X
Inactivated card-keys or inadequate locks on doors to sensitive areas	X	X	X
Keys and card-keys not properly controlled		X	X
Inactivated detection or video surveillance devices		X	X
Video surveillance devices not monitored	X	X	X

Individuals Allowed Access to Sensitive Areas Without Proper Background Investigations

Our review found that security personnel in DEA field locations had not completed background investigations on contract cleaning and maintenance employees working in the facilities. Because these individuals were allowed to work unescorted throughout the offices, they had regular access to areas where sensitive data were routinely handled, processed, and stored on computers. For example, in Division B, the Executive Director of a DEA-led interagency drug task force told us that no background investigations had been conducted on the janitorial personnel who regularly worked in the task force offices. The task force, which is headed by DEA and comprised of law enforcement personnel representing seven federal agencies, as well as other local law enforcement organizations, uses computers to process highly sensitive information on undercover drug smuggling and money laundering investigations.

In another case, preliminary security checks conducted on individuals employed by a maintenance contractor working in Division B showed that one of the workers had a criminal record. The individual's record included, among other offenses, arrests for possession of controlled substances and receipt of stolen property. The division security officer told us he was not aware of the individual's prior criminal record until we pointed it out because the required investigative work, necessary to determine whether any of the contractor employees posed a security risk, had not been

completed. According to the security officer, the contractor employees had been working unescorted in division offices for about a month.

In response to the national security weaknesses we found earlier in our review at the agency, DEA issued guidelines in December 1991 emphasizing the importance of background investigations for contractors working in DEA facilities. However, while these guidelines are a step in the right direction, they will not fully resolve the problems we identified. Specifically, these guidelines are discretionary with respect to the level of background investigation required for all contractors. Moreover, the guidelines do not require full background investigations for contractor cleaning and maintenance personnel, nor do they specifically preclude such individuals from having unescorted access after normal business hours at DEA facilities where national security and sensitive information is processed and stored.

Physical Security Measures Are Inadequate

Physical security safeguards, such as locks, electronic card-key devices, and video surveillance systems, were also not working or were not properly used to control access into and throughout DEA facilities at all three locations. For instance, we found deactivated card-key devices on doors to stairwells, allowing access to all floors. We also found open or unlocked doors to areas where sensitive computers are used and sensitive documents are maintained. In Division A, master card-keys to sensitive areas were routinely made available to non-DEA employees, such as janitors, who worked unescorted in the facility after regular business hours.

We also found cameras and video surveillance devices, designed to monitor activity in and around DEA facilities, that were inoperable. In other cases where such devices were operational, DEA personnel, responsible for monitoring security, did not regularly watch this equipment. For example, Division B video surveillance equipment was not positioned so it could be easily viewed by DEA personnel, and recording mechanisms for storing and replaying video surveillance information were not available. In Division A, the person responsible for watching video surveillance equipment acknowledged spending less than 5 minutes of an 8-hour shift monitoring the equipment due to other work priorities.

Poor Physical Security Practices Pose Serious Risks to Ongoing Investigations

One case at Division A exemplifies how lax physical security can expose sensitive information on ongoing criminal drug investigations to unauthorized disclosure and potential compromise. In this particular case, a computer system, which contained sensitive pen register data used by agents to monitor suspected drug traffickers' telephone calls,[2] was located in a room that was not secured because of a broken lock on the door. We noted numerous DEA employees, as well as unescorted maintenance personnel, entering the room while it was unoccupied. We were also told that janitorial personnel routinely worked unescorted in the room both during and after regular business hours.

The threat posed by these security weaknesses was heightened because the password to the computer system, as well as instructions on how to retrieve system data, had been left beside the computer. Moreover, specific case information was also exposed to compromise because the name, phone number, and DEA case number of an individual under investigation were left taped to the computer screen.

Failure to Control Computer Equipment Poses Additional Risks

DEA also lacks adequate controls to ensure the proper handling and use of computers containing sensitive information. For example, DEA has been unable to develop an accurate and comprehensive inventory of the several thousand microcomputers that its personnel use to process sensitive data. In addition, lax computer maintenance practices and a failure to comply with DEA policy prohibiting the use of personally owned microcomputers for processing and storing sensitive data poses added risks to DEA's sensitive computer information. The locations where we identified these weaknesses are summarized in table 3.3.

Table 3.3: Weaknesses in Controlling Sensitive Computer Equipment at DEA Headquarters and Divisions

	DEA Headquarters	Division A	Division B
Computers not accurately accounted for	X	X	X
Computer fixed-disks not sanitized prior to being released to non-DEA personnel		X	
Personally owned computers used by both DEA and non-DEA personnel		X	X

[2]Pen registers provide an automated method for tracking telephone numbers dialed from a particular telephone for investigative purposes.

Computer Equipment Inventories Are Inaccurate and Incomplete

DEA is unable to account for the several thousand microcomputers its employees use and, therefore, cannot ensure that this equipment is safeguarded against loss or unauthorized use. Since 1988 the agency has been unable to develop an accurate and complete inventory of DEA computers. A December 1991 DEA Office of Inspections report stated that DEA's microcomputer inventory was grossly inaccurate and incomplete because of "lackadaisical" agency record-keeping and poor follow-up in reconciling known computer equipment discrepancies. According to the report, these problems were long-standing and they remained unresolved despite being first reported by DEA internal inspectors in July 1988.

Our review showed that these weaknesses still exist. At Division B, for example, DEA administrative personnel could not account for all computer equipment because property records were not updated to identify where the equipment came from or to whom it belonged. The personnel were also not appropriately updating property records to include new DEA computer equipment purchases. Administrative personnel told us they were unable to devote enough time to preparing and reconciling division computer inventories because of their many other duties.

Without an accurate inventory of computers, DEA cannot track their use and ensure that appropriate safeguards are in place to protect the sensitive information processed on them. Moreover, DEA may not be aware of the loss or theft of computers containing sensitive information.

Lax Computer Maintenance Practices Expose Sensitive DEA Data

During our review, we found three instances in which either Division A or Division B released Office Automation system or microcomputer fixed-disk storage computer equipment to contractor service personnel without first checking to see whether the equipment contained sensitive information. While we were told that the defective fixed disks in two of the cases did not contain sensitive information, in one case, officials from a district office of Division A told us that a defective fixed disk, which had not been sanitized, had been given to a service contractor who replaced it with a new disk in August 1990. This fixed disk had been regularly used to process and store sensitive data, including DEA reports of ongoing drug investigations.

The Department of Justice issued a departmentwide directive in December 1990 controlling the release of fixed-disk computer equipment to contractors. This is because contractors often replace failed computer fixed disks with new disks and then resell the repaired equipment to

others. Therefore, sensitive data left residing on a fixed disk could potentially be accessed by a subsequent user of the repaired equipment. As we testified in March 1991, the vulnerabilities posed by such a release of computer fixed disks to nongovernment sources were graphically illustrated by the sale of surplus Department of Justice computer equipment, containing sensitive grand jury material and information regarding confidential informants, by the U.S. Attorneys Office in Lexington, Kentucky.[3]

However, during our review we found that DEA was still not using proper equipment for removing sensitive data from failed microcomputer fixed disks. During an October 1991 on-site inspection of DEA's microcomputer center where failed fixed disks are repaired, the contractor service technician responsible for sanitizing computer disks was unable to remove data from the disks because the center did not possess the proper sanitizing equipment. This equipment, as stated by the manufacturer, was for removing electronic images from display screens, not for removing data from computer fixed disks. As of March 1992, DEA was still using this inappropriate equipment.

Finally, because of poor record-keeping, DEA was unable to accurately account for all microcomputer fixed disks that have been sent from DEA offices for repair, returned to service contractors, or destroyed. The official responsible for overseeing microcomputer equipment repairs at DEA headquarters told us that this situation exists because documenting the handling and disposition of fixed-disk equipment is not required.

Use of Personally Owned Computers Violates Agency Policy

DEA policy prohibits the use of personally owned microcomputers for processing and storing sensitive data. However, we found that individuals in Division A and Division B were violating these policies. For example, at a DEA-led interagency drug task force in Division B, DEA agents, as well as personnel from other law enforcement agencies, routinely processed and stored sensitive investigative data on their personally owned microcomputers. As a result, sensitive data contained in these computers could be compromised if the equipment, which is outside DEA's control, is stolen, sold, or misused. Failure to control the use of personally owned computers also exposes DEA to computer viruses that may reside in computers owned by individuals. The Executive Director of the task force said he was unaware of Justice's policy and the risks posed by employees using personally owned computers. After our discussions, he took

[3]Justice's Weak ADP Security Compromises Sensitive Data, (GAO/IMTEC-T-91-7, Mar. 21, 1991).

immediate action to prohibit task force members from using personally owned computers.

Computer Security Weaknesses Exist at Other DEA Locations

While our review involved DEA headquarters and offices of two divisions, compliance reviews completed by Justice's Security and Emergency Planning Staff have also found many of the same computer security weaknesses at seven DEA field locations. For example, the compliance review teams found weak security measures to protect sensitive computer systems and data. These weaknesses included poor controls over computer passwords and documents and floppy diskettes containing sensitive information, as well as individuals who were storing sensitive information on unprotected computer fixed disks. The compliance review teams also found physical security deficiencies such as deactivated card-key locks; unlocked doors; and janitorial and maintenance personnel, lacking proper security clearances, who were working unescorted in sensitive areas. Finally, the reviews pointed out the need for full-time designated security officers who are adequately trained and who devote the necessary time to implementing security policies at DEA field offices. DEA has acknowledged the weaknesses found by the compliance review teams and said it is taking action to correct them at these locations.

Weak Internal Controls Permitted Unauthorized Disclosure of Sensitive Computer Information

DEA's Office of Professional Responsibility (OPR) investigates allegations of misconduct by DEA employees, including instances in which it is alleged that sensitive computer information has been disclosed to unauthorized individuals outside the agency. We reviewed 105 preliminary or full investigations of alleged unauthorized disclosure closed by OPR between 1984 and 1991. Of these closed investigations, we found 18 instances in which DEA employees and non-DEA personnel with authorized access to DEA computer systems had obtained sensitive information for unauthorized purposes. In eight of these cases, individuals obtained sensitive law enforcement information that they had no need to know. These instances occurred because DEA has not instituted controls that prevent individuals with access to DEA computers from obtaining data outside their areas of responsibility. Because DEA does not routinely review available computer system audit trail information that could be used to detect improper access and use of sensitive computer data, the agency learned of these security breaches through drug investigations, informants, and other DEA employees.

Justice directives require sensitive computer systems to have established safeguards to restrict access to only those individuals who are authorized and have a need to know information contained in these systems. However, we found eight instances in which individuals, both DEA employees and non-DEA personnel, obtained sensitive computer information, such as NADDIS investigative records, that they did not have a need to know. These individuals then used the information improperly for personal reasons or disclosed it to unauthorized individuals outside the agency. Several of these instances are discussed below.

- A DEA computer course instructor accessed a sensitive computer system and obtained criminal history information on individuals for her own personal use. Specifically, the instructor obtained this information to determine the criminal background of her tenant and her tenant's friend. The instructor further directed a subordinate to obtain and print criminal history information on the tenant's friend from a sensitive computer system.
- A DEA communications equipment operator obtained sensitive criminal investigative data from NADDIS and admitted to unlawfully disclosing the information to a drug trafficker under investigation by DEA. DEA was told that the drug trafficker had paid the communications equipment operator for the information.
- A foreign service national working in a DEA foreign office was given unauthorized access to the NADDIS system over a 2- to 3-year period in violation of DEA policy. DEA personnel improperly allowed this individual to obtain sensitive criminal investigative information from NADDIS.
- A contractor data analyst accessed sensitive NADDIS investigative information outside of her official duties. Specifically, the analyst obtained sensitive information on an ongoing investigation of an individual she was dating.

We believe these instances occurred because DEA does not have adequate internal controls to prevent individuals from obtaining computer data outside their areas of responsibility. For instance, DEA uses passwords and user identifications to restrict access to the NADDIS computer system. However, once an individual is permitted entry into NADDIS no other controls exist to further restrict that person from accessing the many thousands of sensitive drug investigative records that are contained in the system's extensive data files. Without these controls, individuals with NADDIS system access are free to obtain any system data regardless of the information's sensitivity and the individual's need to know. Also, as previously noted, DEA does not routinely analyze available system audit

trail data that record who accesses information in the NADDIS system, when and where the request for information is made, and what information is requested. DEA's Security Programs Manager told us that he does not have sufficient staff to perform such analyses and he questioned its value from a cost/benefit perspective.

Security Weaknesses Need to Be Disclosed Under the Federal Managers' Financial Integrity Act

Under the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512), agencies must establish internal controls to reasonably ensure that agency assets are effectively controlled and accounted for. Agencies must also annually report weaknesses in these controls and the status of any corrective actions. Policies implementing the act further require agencies to incorporate security controls that address the use of their automated information systems.

The extensive security weaknesses we found reflect DEA's failure to execute an effective agencywide computer security program and to ensure that adequate safeguards are established for properly protecting DEA computer systems and the sensitive data they process. Given the risks posed to DEA, these computer security deficiencies constitute serious control weaknesses, which require disclosure and corrective actions under the provisions of the Federal Managers' Financial Integrity Act.

Conclusions and Recommendations

DEA has not fully complied with federal requirements to ensure that sensitive information processed on computer equipment is protected from unauthorized access and disclosure. Moreover, DEA has serious computer security weaknesses that pose significant risks to the agency's computer systems and the sensitive data they contain. This disturbing situation exists because the agency has not implemented an effective computer security program. Such a program should provide those security controls necessary to ensure the protection of all of DEA's sensitive computer systems and the data they contain. Specifically, DEA has not identified and prepared security plans for all of its sensitive computer systems, nor has it completed all required contingency plans or risk analyses. Further, DEA has not taken adequate action to ensure that all DEA personnel are aware of their security responsibilities and how to fulfill them. Moreover, DEA does not effectively monitor and enforce computer security. Finally, while Justice's oversight is improving, the department also needs to work more closely with DEA to ensure that the agency complies with all federal and departmental computer security requirements.

Recommendations

DEA's failure to fully comply with federal computer security requirements and the disturbing computer security weaknesses we found pose serious risks that potentially hinder DEA's mission and threaten the lives of federal agents. To address these risks, the agency must take immediate action to ensure that the sensitive information it processes and stores on computers is adequately protected.

We therefore recommend that the Attorney General direct the Administrator of the Drug Enforcement Administration to:

(1) Establish and implement an agencywide computer security program as required by Justice and other federal directives. As part of this program, DEA should ensure that all sensitive computer systems are properly identified and that security plans are prepared and implemented for each of these systems. To adequately protect its sensitive computer systems and facilities, DEA should also ensure that thorough risk analyses are conducted for all sensitive computer systems and any identified weaknesses are corrected, contingency plans are tested and implemented, and all employees are made aware of federal and agency computer security requirements and how to fulfill them.

(2) Strengthen DEA's monitoring and oversight of computer security. Specifically, DEA should issue clear and specific requirements for

designated security officers to follow in monitoring and enforcing computer security. Also, Office of Security Programs should train its staff in computer security and conduct more thorough security surveys that effectively identify and correct vulnerabilities.

(3) Ensure that computer security weaknesses identified in this report are corrected and that similar weaknesses do not exist elsewhere. At a minimum, DEA needs to control access to areas where sensitive data are processed and stored; adequately protect computer data, including the establishment of safeguards to restrict data access to individuals having a need to know; collect and review computer audit trail information to detect improper access to and use of sensitive computer data; and ensure that computer equipment used to process and store sensitive information is properly accounted for and controlled. Moreover, DEA should take appropriate steps to ensure that sensitive data are removed from computer equipment released outside of the agency for repair or disposal.

(4) Report the computer security deficiencies we found as material internal control weaknesses under the Federal Managers' Financial Integrity Act.

In addition, we recommend that the Attorney General direct the Justice Management Division to work closely with DEA to ensure that the agency implements the above recommendations and complies with all federal and departmental computer security requirements.

As requested, we did not provide a draft of this report to Justice and DEA for review and comment. However, we discussed the report's contents with Justice's Assistant Attorney General for Administration and DEA's Assistant Administrator for Planning and Inspection, who generally agreed with the facts presented. We have incorporated their views in the report as appropriate.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.	Stephen A. Schwartz, Assistant Director William D. Hadesty, Technical Assistant Director Mark D. Shaw, Evaluator-in-Charge Richard L. Sumner, Senior Evaluator B. Gail Moore, Senior Evaluator Kurt A. Burgeson, Staff Evaluator Shane D. Hartzler, Writer-Editor
Office of General Counsel	Richard Seldin, Senior Attorney

Ordering Info