GAO

United States General Accounting Office

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

February 1992

COMPUTER SECURITY

DEA Is Not Adequately Protecting National Security Information

RESTRICTED--Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations.

GAO/IMTEC-92-31

GAO

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

Information Management and
Technology Division

B-246961

February 19, 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, we are currently reviewing the Drug Enforcement Administration's (DEA) computer security. Although our review is focused on the security of DEA computer systems processing sensitive information,[1] we have identified serious weaknesses involving national security information[2] at DEA headquarters and two of the agency's larger field divisions, hereafter referred to as Division A and Division B. Because of the seriousness of the weaknesses, we provided the Attorney General with a Limited Official Use report on January 9, 1992, identifying the specific locations where security deficiencies were found so corrective action could be immediately taken. 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 national security information that the agency has an obligation to protect. Our related work on the security of DEA computer systems processing sensitive information is continuing and we will report to you on that work at a later date. For additional information on our objectives, scope, and methodology, see appendix I.

Results in Brief

DEA is not adequately protecting national security information processed on its computer systems.[3] Although DEA officials said they know of no instance where such information has been compromised, unauthorized access to and disclosure of this information could possibly endanger lives, undermine ongoing law enforcement investigations, and ultimately

[1]According to the definition of terms stated in the Computer Security Act of 1987 (15 U.S.C. 278g-3(d)(4)), sensitive information is 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]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 the national security.

[3]As agreed with DEA, we did not read the information contained in computer systems and other materials except to identify that it was information DEA has designated as classified.

jeopardize the nation's war on drugs. This disturbing situation exists because DEA has failed to adequately control and provide needed safeguards for computers processing national security information.

Background

The Drug Enforcement Administration was established in 1973 under the Department of Justice to enforce laws and regulations relating to the use and distribution of legal and illegal drugs. The agency accomplishes its mission through an organization consisting of about 7,000 agents and other employees, with headquarters and domestic and foreign offices located worldwide.

To carry out its mission, DEA relies on computer systems to process highly sensitive and national security information collected from a variety of sources. Such information includes detailed data on known or suspected drug violators and informants, as well as data on domestic and international drug operations, and gathered intelligence. Unauthorized disclosure of this information could possibly disrupt DEA operations and adversely affect the nation's war on drugs.

Executive Order 12356, dated April 2, 1982, requires federal agencies to establish controls for ensuring that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that provide adequate protection and prevent access by unauthorized persons. In addition, Justice policy requires that its component agencies, including DEA, ensure that adequate security safeguards are in place for protecting computer systems that process national security information.[4]

Computers That Process National Security Information Not Identified by DEA As Required

Department of Justice policy requires its component agencies to identify all computer systems, including microcomputers, that process classified data.[5] These systems must be identified so that the information contained in them can be adequately protected from unauthorized disclosure and compromise. However, DEA has not identified all its computers that process classified information, in compliance with Justice's policy.

In February 1991, DEA informed Justice that it had an inventory of computers that process classified information. DEA's inventory was prepared

[4]U.S. Department of Justice, Automated Information Systems Security (DOJ 2640.2B), Nov. 16, 1988.

[5]U.S. Department of Justice, Automated Information Systems Security Bulletin Number 2, Sept. 8, 1989.

on the basis of a survey conducted by the Office of Security Programs. However, at the time of our review, we found that this inventory was not complete. Specifically, the inventory did not include computers that headquarters and Division B use to process classified data because (1) headquarters offices were never surveyed and (2) Division B did not respond to requests for this information. Moreover, Division A did not report any classified computer systems in response to the survey when, in fact, we found that division personnel were using computers to process classified information. Without knowing how many and which computers process classified information, DEA cannot ensure that adequate safeguards are in place for protecting national security information.

Use of Unapproved and Unprotected Computer Equipment Poses Serious Risks

National security guidelines point out that most computer systems processing classified information do not have sufficient controls for preventing someone from accessing information stored within the system.[6] Therefore, proper access controls must be implemented to safeguard this information. In accordance with federal guidelines, Justice policy requires that computer systems processing classified information be approved by the Department Security Officer and have the necessary safeguards in place for ensuring adequate security.[7] These safeguards include, but are not limited to, performing risk analyses to evaluate security threats, operating the computer systems in a controlled environment, and ensuring that appropriate security measures are in place, which for example, could include the use of equipment that complies with TEMPEST requirements.[8] Justice policy also requires that adequate communications security safeguards be established for protecting classified data transmitted on computer networks between workstations.

Contrary to these guidelines, we observed many instances in which headquarters and division personnel were improperly using DEA's Office Automation system, a network system that has not been approved or appropriately safeguarded for processing national security information, to routinely process classified data. DEA has not completed a risk analysis of the system. Further, Office Automation workstations are operated in open, unshielded work areas, and the equipment is not TEMPEST-protected.

[6]National Telecommunications and Information Systems Security, Office Automation Security Guideline, Jan. 16, 1987.

[7]DOJ 2640.2B, Nov. 16, 1988 and Automated Information Systems Security Bulletin Number 2, Sept. 8, 1989.

[8]TEMPEST is a technology that shields computer equipment to keep electromagnetic emissions from being intercepted and deciphered by eavesdroppers.

Moreover, we were told by the Chief of the Office Automation Section that workstations are connected by data communications lines that are not encrypted, a violation of national security guidelines and Justice policy. Therefore, unauthorized individuals can intercept or monitor information emanating from and transmitted by the Office Automation system without being detected.[9]

The improper use of the Office Automation system to process classified information presents additional risks of unauthorized access. For example, we noted that the Office Automation network allows individuals working on workstations in one office to access data stored in workstations located elsewhere and used by others. Therefore, any DEA employee using the system, who may lack the necessary security clearances and a valid "need to know", can obtain classified data stored in another employee's workstation without that employee's knowledge. In addition, we were told by several DEA officials that employees of the original equipment vendor have access to Office Automation workstations because the vendor-issued system passwords have never been changed, even though DEA began installing the Office Automation system in 1987.

Also, DEA personnel were processing classified information on the Office Automation system and microcomputer equipment with fixed-disk storage devices in open, unshielded work areas. Federal guidelines recommend against using this type of equipment because, unknown to the system user, information may be inadvertently stored on the computer's fixed disk, leaving it vulnerable to retrieval by unauthorized persons. Instead, the guidelines state that if computer systems are used to process classified information in open areas, computer equipment with removable-media-only should be used. The importance of safeguarding against the inadvertent storage of information on fixed disks was graphically illustrated by the sale last year of surplus Department of Justice computer equipment, which contained sensitive grand jury material and information regarding confidential informants, by the U.S. Attorneys Office in Lexington, Kentucky.[10]

[9]Computer Security Studies Have Shown That Eavesdroppers Using Relatively Unsophisticated and Inexpensive Equipment Can Effectively Detect and Reproduce Data From Computer Display Screens Located on Desk Tops in Remote Buildings.

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

Physical Security Weaknesses Further Jeopardize National Security Information

Physical security weaknesses at DEA compound the serious computer security problems discussed above. We found that DEA is not adequately controlling access to areas where computers process national security information, and classified computer-generated materials and documents are not being properly safeguarded. These weaknesses are summarized in table 1.

Table 1: Physical Security Weaknesses at DEA Headquarters and Divisions

	DEA Headquarters	Division A	Division B
Inadequately controlled access to sensitive areas	X	X	X
Individuals without national security clearances working unescorted in sensitive areas	X	X	X
Unattended computers left signed on[a]	X	X	X
Computer-generated materials left unattended and unsecured		X	X
Documents left unattended and unsecured	X	X	X
Safes left open and unattended	X	X	

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

Inadequate Controls Over Access to Areas With National Security Information

We found weaknesses in DEA's procedures for controlling access to areas where computer equipment is used. As a result, unauthorized personnel, lacking appropriate clearances or a valid "need to know", have direct access to classified information. For example, at headquarters and the two division offices, contract cleaning and maintenance personnel, who do not have national security clearances, were allowed to work unescorted in areas where computers process national security information. In fact, at both division offices, janitorial staff were permitted to work alone in these areas both before and after regular business hours. We also observed that computers in each of these offices were often left signed on and unattended, allowing unauthorized individuals access to the data contained in these systems.

We also found inadequate physical safeguards for controlling the entry of individuals to areas that contain national security information. At Division A, for example, electronic card-key devices on doors to areas that contained national security information are turned off during normal working hours and the doors left open. Moreover, the division security staff are not reviewing the card-key access logs to determine if unauthorized attempts

were made after normal working hours to gain entry to areas where classified information was collected, processed, and stored. In fact, our review of the card-key access logs showed that one card-key that had been reported lost was still active, and individual card-keys with the same access codes had been issued to groups of individuals, including non-DEA employees. Further, DEA employees do not wear security badges, making it difficult to determine if unauthorized personnel are entering sensitive areas.

Division B also had serious entry control weaknesses. At the time of our review, for example, locks to the division offices had not been changed since being installed in 1985, despite the fact that DEA and task force employees reported 17 instances since then in which their keys were either lost or stolen. These instances included the loss of master keys to all areas where computers process national security information and where employees regularly collect, analyze, and store this information. In one case, an employee reported the loss of office keys on a key chain containing the initials DEA. According to the Division Security Officer, the locks to the division offices are being rekeyed. DEA's Assistant Administrator for Planning and Inspection also told us that this division is being relocated to new space that will be equipped with a card-key system.

Classified Computer-Generated Materials and Documents Not Safeguarded

We also found security weaknesses in the methods by which DEA personnel handle computer-generated materials and documents containing national security information. For example, at both divisions, floppy diskettes labeled as containing classified information were routinely left unattended in open and unprotected mail trays, which is contrary to DEA policy. These trays were within easy access to anyone, including non-DEA personnel who were working unescorted in the facilities. At DEA headquarters, we observed several instances in which documents labeled as classified were left unsecured in areas where unescorted cleaning personnel, lacking national security clearances, were working. In one case, classified-labeled documents were left out and unattended on a desk next to a window on the first floor. After confirming with a DEA employee that the documents were classified, we returned to the location 5 minutes later, only to find that the documents had again been left unattended.

In another case, we observed a secure facsimile machine, located in an unsecured area, with what we were told was a classified document lying unattended in the machine tray. The area was an open mail room where non-DEA personnel (contractors) regularly work.

In addition, we found many instances at DEA headquarters and at division offices where documents labeled as classified were left unattended in open cubicles and in unlocked offices. We also observed safes acknowledged by DEA personnel as containing national security information that were left open and unattended.

National Security Weaknesses Exist Elsewhere

Although our review was limited to the three locations discussed above, the Department of Justice recently found similar national security weaknesses at another major DEA field location. During a security compliance review completed by Justice's Security and Emergency Planning Staff in August 1991, the review team found that (1) DEA personnel were processing and storing national security information on unapproved and unprotected computer equipment, (2) communications lines connecting remote workstations were not safeguarded in accordance with national security requirements, (3) individuals with access to sensitive areas did not have proper security clearances, and (4) access to the Sensitive Compartmented Information Facility that houses highly classified information was not properly controlled.

DEA has acknowledged these weaknesses and is taking action to correct them at this location. For example, DEA is working with Justice's Security and Emergency Planning Staff to establish adequate security controls over computers used at this location to process classified information.

Conclusions

DEA is not complying with federal requirements to ensure that national security information processed on computer equipment is protected from unauthorized access and disclosure. DEA does not know what computers are being used to process national security information, and personnel are routinely processing classified information improperly on computer equipment that is not approved for such use or is not appropriately safeguarded.

Lax physical security practices make these weaknesses even more disturbing. Access to areas where computers process national security information is not adequately controlled and non-DEA employees lacking security clearances, such as janitors, are allowed to work unescorted in these areas. In addition, floppy diskettes and classified documents containing national security information are left unsecured. These problems are not limited to the locations we visited. The Department of Justice has found similar national security weaknesses at another important DEA field location.

Although DEA officials said they know of no instance where national security information has been compromised, these disturbing security weaknesses pose serious risks that could potentially hinder DEA's mission and threaten the lives of federal agents. Therefore, the agency needs to take immediate action to ensure that the national security information it processes and stores is adequately protected.

Recommendations

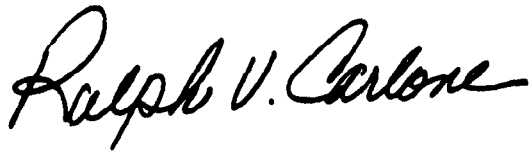
As stated in our earlier report to the Attorney General, we recommend that he direct the Administrator of the Drug Enforcement Administration to immediately correct the security weaknesses described in this report. Specifically, at DEA headquarters and the two divisions we reviewed, the Administrator should identify all computers processing national security information, perform risk analyses to assess security threats, and establish appropriate security safeguards as needed in conformance with federal requirements. This should include ensuring that (1) adequate controls are in place over access to areas where national security information is processed and stored and (2) DEA employees are made aware of their responsibility to appropriately safeguard national security information.

In addition, the Administrator should determine whether similar national security information weaknesses exist at other DEA domestic and foreign locations, and take the required corrective action, as discussed above, where necessary.

Our work was conducted between June and December 1991, in accordance with generally accepted government auditing standards. The views of responsible officials were obtained during the course of our review and are incorporated where appropriate. As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies to the Attorney General of the United States; the Administrator, Drug Enforcement Administration; the Director, Office of National Drug Control Policy; the Director, Office of Management and Budget; and to other interested parties. We will also make copies available to others upon request.

This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who can be reached at (202) 336-6418. Other major contributors are listed in appendix II.

Sincerely yours,



Ralph V. Carlone
Assistant Comptroller General

Objectives, Scope, and Methodology

In response to a request from the Chairman, Government Information, Justice, and Agriculture Subcommittee, House Committee on Government Operations, we are reviewing DEA's computer security. The objectives of our review are to determine (1) if DEA is complying with the Computer Security Act of 1987 and other federal policies and procedures, (2) the risks associated with any deficiencies found, and (3) whether the Department of Justice is overseeing DEA's compliance with the Act and other federal guidelines. Although our review is still underway, we identified serious computer security weaknesses involving national security information. This report discusses these security weaknesses, and in particular whether DEA has complied with federal requirements for protecting national security information. We did not review the adequacy of DEA's safeguards over its Secure Mail System and over the Sensitive Compartmented Information Facilities the agency operates. Our work relating to the security of DEA sensitive computer systems is continuing, and we will report to the Chairman on that work at a later date. As agreed with DEA, we did not read the information contained in computer systems and other materials except to identify that it was information DEA has designated as classified.

To assess DEA's efforts to comply with national security requirements, we examined its policies and procedures for safeguarding national security information. In addition, we interviewed DEA personnel who use computer systems to process classified information at DEA headquarters and at the offices of two of its larger field divisions. To assess the adequacy of existing security safeguards, we reviewed physical and computer operations security at headquarters and at the two divisions. Our work included observing physical security practices followed by DEA personnel and reviewing the security safeguards used to protect national security information that is processed on DEA's Office Automation system and other microcomputer equipment.

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 Information

The first copy of each GAO report is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100