United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Crime and Criminal Justice, Committee on the Judiciary, House of Representatives

May 1991

WAR ON DRUGS

Information Management Poses Formidable Challenges

144274

GAO/IMTEC-91-40

GAO

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

Information Management and
Technology Division

B-243484

May 31, 1991

The Honorable Charles E. Schumer
Chairman, Subcommittee on Crime
and Criminal Justice
Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

You asked us to identify automated information systems used by federal agencies in combatting illicit drugs. In April, we provided you with two separate reports—one classified and one For Official Use Only—discussing the results of our counterdrug systems inventory. You also asked us to (1) determine the status of the federal drug control community's efforts to improve counterdrug information management, and (2) identify issues facing it in this endeavor. This report provides this information. Additional information on our objectives, scope, and methodology is contained in appendix I.

Drug use is flourishing in the United States. Drug-related crime and violence has reached alarming heights. In response to this crisis, the Congress created the Office of National Drug Control Policy (ONDCP) in 1988 to develop a national drug control program and oversee the federal drug control fight. But trying to stop the drug trade is incredibly complicated and requires the effective exchange of information among many federal agencies. There are huge geographical distances that must be patrolled, and thousands of vehicles, airplanes, and boats that enter the United States every day, and well-financed drug smugglers who can adapt to enforcement efforts.

Results in Brief

Currently, 24 civilian and intelligence agencies and 9 Department of Defense (DOD) components operate over 100 drug control information systems. Effective management and sharing of the enormous amount of information in these agencies' automated systems is critical to how well the government wages its war on drugs. Through its interagency working groups, ONDCP is assessing the information needs and capabilities of federal agencies involved in drug control to formulate a master plan for promoting better use and sharing of drug-related information.

ONDCP is also overseeing specific short-term communications improvements at the agencies. However, formidable challenges must be overcome before the administration's information management goals can be accomplished.

First, central information resources management (IRM) leadership is needed for directing agencies with drug control missions to commit the resources and take the actions necessary to improve the use and sharing of drug-related information. Currently, no one entity, including ONDCP, has clear authority for carrying out this responsibility. Instead, since each agency determines how its information resources are funded and used, we are concerned that, without central IRM leadership, a disjointed, agency-by-agency approach to counterdrug information management will occur, thereby hindering rather than promoting needed improvements. Second, incompatibilities among agencies' systems pose interoperability problems, meaning some systems cannot work together to exchange information. For example, the lack of interoperability between systems used by the Drug Enforcement Administration and other agencies has, in some cases, delayed the exchange of time-critical investigative data.

Third, data integrity problems must be solved—sharing inaccurate or unreliable information could misdirect interdiction efforts and incriminate innocent persons. For example, design deficiencies in the Customs Service's system for detecting and tracking drug smugglers has caused the system to associate flight plans with the wrong aircraft and to share the wrong information with other law enforcement authorities. Fourth, systems need to do a better job of protecting sensitive data about people, investigations, and national security. For instance, the Department of Justice has failed to protect sensitive information about informants and undercover agents.

Finally, the proliferation of intelligence centers greatly complicates the management of this information. Over 30 centers now exist and more are planned. As the number of centers increases, coordinating operations and sharing information becomes increasingly complex.

ONDCP hopes to begin addressing three of these issues—interoperability, data integrity, security—and aspects of the fourth issue—managing the proliferation of intelligence information—as part of its overall master plan scheduled to be completed later this year. However, this work is far

from complete, and it is not clear whether the plan will provide a workable framework from which to adequately resolve these issues. Moreover, it is not clear how ONDCP intends to address the need for leadership, which is necessary for ensuring that the agencies fund and implement IRM improvements called for in the master plan. Therefore, we are recommending that, in developing its master plan, ONDCP set clear, measurable objectives and time frames for resolving all five of the issues discussed here. Regarding leadership, ONDCP must establish its information system goals, define mechanisms for resolving conflicts that may occur with agencies' primary mission goals, and ensure adequate funding and implementation of drug information programs. We also recommend that the Director report to the appropriate committees within Congress on ONDCP's plans for addressing the five issues and regularly report on the progress made toward resolving them.

Background

Countering the supply of illegal drugs—that is, the cultivation, production, transportation and distribution of drugs—requires concerted federal agency action and maximum use of all the government's resources. In response to the growing domestic drug threat, the Congress passed the Anti-Drug Abuse Act of 1988 (P.L. 100-690). Under this act, ONDCP was created within the Executive Office of the President to develop a national drug control program and to oversee and coordinate the federal drug fight. Among other things, the act requires the Director of ONDCP to

- establish policies, objectives, and priorities for the national drug control program;
- promulgate an annual National Drug Control Strategy;
- advise the President regarding necessary changes in the organization, management, budgeting, and personnel allocation of federal agencies involved in drug enforcement; and
- notify federal agencies if their policies are not in compliance with their responsibilities under the national drug control strategy.

Since its inception, ONDCP has prepared and the President has issued the administration's National Drug Control Strategy (consisting of three companion volumes dated September 1989, January 1990, and February 1991). Generally, the strategy explains the nature of the drug crisis in America and sets forth what the administration calls a comprehensive

plan for targeting the drug problem on multiple fronts, such as treatment, international initiatives, and border interdiction.[1] Although ONDCP does not direct agencies to carry out specific actions, ONDCP does encourage them to adopt initiatives that the administration believes are necessary to reduce the level of illegal drug use in America. For example, ONDCP has established numerous committees and working groups made up of representatives from agencies with drug control responsibilities. Through these interagency groups, ONDCP seeks to build consensus among the agencies in order to accomplish strategy goals.

In addition, to carry out its budget responsibilities under the Anti-Drug Abuse Act of 1988, ONDCP has implemented an annual drug budget process for monitoring and reporting the obligation and expenditure of federal drug funds. As part of this process, ONDCP certifies whether agency budget requests meet the goals of the strategy. However, it should be noted that the agencies themselves ultimately decide how their resources are actually used.

According to ONDCP's National Drug Control Strategy Budget Summary, the Administration is spending an estimated $10.5 billion on the drug problem during fiscal year 1991, and it has requested an estimated $11.7 billion for fiscal year 1992. A large part of the funds identified in the drug budget are being used for the interdiction and enforcement activities of over 25 organizations that make up the federal drug control community, including law enforcement agencies, national foreign intelligence agencies, and the Department of Defense (DOD). Agencies that have major counterdrug responsibilities are listed in appendix II, and those with lead counterdrug missions are discussed in appendix III.

As we noted in a report last year, however, drug budget, obligation, and expenditure data are often only estimates and cannot be identified precisely through agency accounting systems.[2] Office of Management and Budget officials said this is because drug programs in agencies are generally not separate accounts but are combined with other programs in an account. In this regard, ONDCP could not provide specific information showing how much each agency actually spends on drug-related automated information systems because such costs are generally included as

[1]The National Drug Control Strategy describes the drug problem in economic terms; that is, as a largely market function influenced by the variable "supply" of drug sellers and the variable "demand" of drug buyers.

[2]Developing a Federal Drug Budget: Implementing the Anti-Drug Abuse Act of 1988 (GAO/GGD-90-104, Aug. 23, 1990).

part of the agencies' overall automated data processing expenditures and these costs are not broken down separately. Despite these difficulties, we recommended that the Director of ONDCP give emphasis to improving the government's capability to identify and track drug expenditure data.

Status of ONDCP Efforts to Improve Counterdrug Information Management

Information plays a critical role in the drug fight. Revealing drug trafficking activities and guiding enforcement efforts depends on how well information is collected, managed, and disseminated among the many agencies actively engaged in drug control. Because of this, the Administration's National Drug Control Strategy calls for ONDCP and the agencies to ensure the effective use and sharing of this important resource. ONDCP is sponsoring two interagency working groups—the Communications Interoperability Working Group and the Automated Data Processing Working Group—which are examining the automated data processing and telecommunication capabilities of the drug control agencies and identifying how to maximize the exchange and use of drug-related information.

These two interagency groups include individuals from the many agencies that play important counterdrug roles. By consensus and by establishing agreed-upon requirements for automated data processing and communications, the groups attempt to coordinate cooperative agency action and encourage agency funding of those initiatives needed for making improvements in counterdrug information management throughout the drug control community.

Interagency Working Groups' Activities

The Communications Interoperability Working Group's purpose is to coordinate the use of secure and interoperable communications systems among drug control agencies.[3] The group, which is chaired by the Coast Guard, is setting communications standards and overseeing agencies' efforts to improve communications. For example, the Border Patrol purchased, on the recommendation of the Communications Interoperability Working Group, very high-frequency radios that are compatible with radios used by other agencies. The group encouraged this in order to improve voice communications among drug control agencies.

[3]Secure communications involve protecting voice and record transmissions against compromise such as unauthorized disclosure. Interoperability is the ability of systems to work together to send and interpret messages, share data, etc.

In December 1990, the group issued revised plans that define requirements needed to ensure more secure and interoperable communications throughout the drug control community. Although the agencies are generally looked upon for funding these requirements, in many instances they do not have the necessary resources available for correcting certain telecommunications shortfalls. In response to this immediate need, the effort was supplemented with congressionally authorized DOD funds managed by the Defense Communications Agency.[4] For example, in fiscal year 1991, DOD will spend about $56 million to fund law-enforcement agencies' purchases of existing technology—interoperable, secure communications equipment—in accordance with the requirements set forth by the Communications Interoperability Working Group. As discussed in the working group's revised plan for fiscal year 1992 and beyond, however, the agencies will have to fund the needed requirements out of their own budgets.

The Automated Data Processing Working Group, which is chaired by the Federal Bureau of Investigation, is studying automated data processing systems and the types of data they contain because comprehensive information on the many systems that support counterdrug work has not been developed. Studies under way focus on identifying automated data processing capabilities and communications connections, describing the flow of data between agencies, as well as examining ways to promote data security, privacy, and integrity in the fusion,[5] storage, and distribution process. In April 1990, the Automated Data Processing Working Group formed various subgroups, obtained contractor support, and began data collection work. The studies are scheduled to be completed by December 1991.

The results of the work being performed by the Communications Interoperability Working Group and the Automated Data Processing Working Group will be incorporated into a single National Information Management and Communications Architecture Master Plan planned for issuance in December 1991. Specifically, ONDCP anticipates using the master plan to prioritize requirements for counterdrug automated data processing and communications improvements. For example, the plan could call for additional system procurements and set new security standards for automated data processing systems across the drug control

[4]P.L. 101-189, Nov. 29, 1989, Section 1204.

[5]Fusion is the blending of intelligence information from multiple sources to produce a single intelligence product.

community. Meanwhile, agencies continue to develop and enhance systems that support their individual information needs.

Agencies Work on Short-Term Automated Data Processing and Telecommunications Improvements

While working toward a master plan, ONDCP has identified some short-term initiatives that it believes will promote better information management and sharing. Generally, these initiatives focus on expanding access to information. They include increasing the use of automation and improving or developing critical automated data processing and telecommunications systems. Generally, these initiatives are being funded through the agencies' own automated data processing budgets. A more detailed discussion of key agency initiatives is provided in appendix IV.

Drug Control Community Faces Formidable Challenges

ONDCP's working groups are making progress toward the development of a master plan for managing and sharing drug information. However, they acknowledge that completing this task poses formidable challenges. We agree. Our work showed that making the best use of information among agencies with differing missions, unique automated data processing and telecommunications capabilities, and their own information management problems, heightens the need for: (1) central IRM leadership; (2) interoperable information systems; (3) data integrity with safeguards for protecting individuals' rights; (4) adequate security over systems that contain classified and sensitive data; and (5) interagency coordination of intelligence information.

Central IRM Leadership Is Needed

In an environment in which more than 25 agencies are pursuing their own mission-related responsibilities, central IRM leadership is needed to ensure cooperative agency action and to successfully implement a governmentwide information management strategy. Individual agencies, where component offices or organizations have varying degrees of independence, provide a good example of the important role leadership plays. Our past work at agencies including the Department of Justice, the Immigration and Naturalization Service, and the Coast Guard, showed that weak central IRM leadership led to incompatible automated data processing systems and a disjointed IRM approach that did not meet the overall goals of the agency and basic user needs.[6]

[6]Coast Guard: Strategic Focus Needed to Improve Information Resources Management (GAO/IMTEC-90-32, Apr. 24, 1990); Information Management: Immigration and Naturalization Service Lacks Ready Access to Essential Data (GAO/IMTEC-90-75, Sept. 27, 1990); and Information Resources: Problems Persist in Justice's ADP Management and Operations (GAO/IMTEC-91-4, Nov. 6, 1990).

In the drug control environment where agencies independently control their own automated data processing activities, central IRM leadership is needed for directing the agencies to commit the resources and implement the actions necessary to meet the Administration's National Drug Control Strategy's goal of improved information management. Currently, no one entity, including ONDCP, has clear authority for carrying out this responsibility. Instead, ONDCP and its working groups attempt to build consensus among the agencies and, through coordination and oversight, attempt to influence agency actions. Ultimately, however, because the agencies themselves decide how their drug-related automated data processing and telecommunications resources will be used, agency IRM officials are concerned that improvements needed for a coordinated national attack on drugs will likely be sacrificed for other program areas considered more important to the principal missions of the agencies. ONDCP officials share these funding concerns, noting that some agencies may not be able to pay for actions called for by the master plan. Unless the plan is fully implemented across all the agencies, its success in bringing about needed improvements cannot be ensured.

Interoperability Problems Inhibit Information Exchanges

Effective drug enforcement depends on the timely and accurate exchange of information between agencies, which requires a high degree of computer interoperability. However, incompatibilities among agencies' automated information systems and their use of data that are not automated limit how well agencies share important drug investigative information.

Our recent inventory report points out that federal civilian, intelligence, and DOD agencies operate or are developing over 100 automated information systems that support counterdrug responsibilities. Many of these systems were originally designed to meet the specific mission needs of individual agencies and have been adapted for counterdrug work. Furthermore, agencies use different vendors' proprietary systems. As a result, one system is often not compatible with another and modifications are needed to allow the systems to share information.

A clear example of this lack of interoperability was pointed out in a recent Justice report on the Drug Enforcement Administration's El Paso Intelligence Center, the drug control community's principal tactical interdiction center.[7] The review found that, because the center's automated data processing environment consists of a collection of disparate

[7]Special Analysis Report El Paso Intelligence Center, Department of Justice (May 1990).

hardware, software, telecommunications, and computer systems, the center uses many special-purpose data base systems that are not interoperable. As a result, the center's data bases can only be accessed through the use of multiple, single-function terminals. This restriction causes analysts to waste time physically moving from one computer terminal to another to complete each investigative search. Furthermore, agencies trying to obtain information from the center find the process time-consuming and not always responsive to their needs.

The use of data that are not automated further restricts timely exchanges of drug investigative information between agencies. For example, Drug Enforcement Administration files containing investigative information on drug suspects and violators are available only on paper. Because of this, personnel have to perform lengthy searches through paper files before important information can be sent to agents in the field. Similarly, a key Coast Guard intelligence system will not electronically accept data. As a result, Coast Guard personnel have to manually enter large amounts of drug data into the system before the information can be analyzed and disseminated to others. Coast Guard officials told us that valuable time and resources are wasted as a result of this manual process.

ONDCP and its working groups acknowledge that such problems exist. Although the Communications Interoperability Working Group has achieved some success with improving the interoperability of voice communications systems, ONDCP has not determined the extent to which interoperability problems currently limit the exchange of drug data. As part of the master plan, ONDCP's working groups are attempting to identify systems that need to be interoperable. Until this work is complete, however, ONDCP will not know the cost or technical complexities of solving interoperability problems that exist between agency information systems that need to share data.

Data Integrity Will Be Difficult to Guarantee

It is vital that the integrity of data used throughout the counterdrug community be assured. Sharing inaccurate or unreliable information could misdirect interdiction operations and incriminate innocent persons. Previous audits have criticized agencies, such as the Drug Enforcement Administration, for using systems that contained erroneous and

old data.[8] Further, no standards exist for determining the quality of data used and shared among the agencies.

We found that data integrity problems continue to plague agencies involved in drug control. For example, the Customs Service is struggling with its Command, Control, Communications and Intelligence system. This system is one of the law enforcement community's primary tools for detecting and tracking drug smugglers entering the United States. However, according to Customs, design deficiencies have caused problems such as the system associating flight plans with the wrong aircraft. Additional problems with the system's flight surveillance capabilities have caused incorrect information to be sent to Customs' law enforcement aircraft and other agencies. In fact, operators continue to use a separate radar system to verify the Command, Control, Communications, and Intelligence system data because they lack confidence in the system. These problems cannot be easily remedied since a contractor dispute has left Customs without the technical specifications necessary for making corrections.

In addition, no standards exist for ensuring data quality across the drug control agencies. As a result, agency officials told us they are sometimes reluctant to act on information they receive from other agencies because they lack confidence that the information is accurate. Agency officials cited a typical case where agency A shares an intelligence message with agency B without verifying that the information is correct. Agency B reformats the message and sends it out to others without indicating the origin of the information. When the reformatted message is circulated back to agency A, personnel may act on the information because they mistakenly believe that agency B has confirmed the information.

In collecting and disseminating information on individuals, the government is legally required to protect people's privacy and their other constitutional rights. The Privacy Act, for example, provides some restrictions on the information agencies can maintain about individuals.[9] Moreover, increased sharing also makes it extremely important to safeguard against deliberate or inadvertent collection and use of data that impinge on individuals' rights. For example, Treasury's Financial Crime Enforcement Network center collects financial information from government and commercial sources to investigate drug money laundering.

[8]See Audit Report: The Drug Enforcement Administration's Automatic Data Processing General Controls, Department of Justice (July 1989).

[9]5 U.S.C. 552 a.

However, the network center is limited in the information it can legally obtain from commercial data bases, by applicable law, such as the Fair Credit Reporting Act.[10]

ONDCP's working groups recognize the need to collect and disseminate accurate and reliable drug information while protecting the rights of individuals. Working group officials said that they are developing a plan for addressing this issue since, clearly, controls for ensuring data integrity throughout the drug control community are needed. However, without clear central IRM leadership as discussed above, we are concerned whether, even with a plan, a consistent and effective set of controls will be accepted and implemented by all the agencies.

Classified and Highly Sensitive Data Need to Be Secure

The drug control community faces challenging security demands. Prudent automated data processing security practices require agencies to protect the classified and highly sensitive data they collect and use. However, serious automated data processing security weaknesses surround the use and sharing of sensitive drug information within and between drug control agencies.

Last year, we found that the Department of Justice was not protecting its highly sensitive computer systems.[11] The Department had many disturbing weaknesses in existing security which, if not corrected, could severely compromise the computer systems and the sensitive information they process. For example, physical and operational controls over computer security were inadequate, contingency plans were not prepared or properly tested, and no computer security training was provided to employees. More recently, we testified on the Department's continuing neglect and inattention to computer security. Specifically, we discussed how serious breaches in security have life-and-death ramifications for individuals whose identities may have been compromised by the exposure of sensitive information.[12]

Besides internal security controls, steps must also be taken to protect information that is transferred to other agencies. For example, Customs Service personnel at the Command, Control, Communications, and Intelligence West center said that network communications between the

[10]Fair Credit Reporting Act, P.L. 91-508, Section 601.

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

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

center and DOD and law enforcement agencies were not secure for approximately 6 months because DOD contractors had improperly installed system equipment. As a result, data contained in and transmitted by the network was vulnerable to access by unauthorized individuals. Agency officials are also concerned about losing control over who has access to their sensitive information when it is exchanged with other agencies. For instance, law enforcement agents said they prefer exchanging certain investigative information by secure telephone rather than entering data into shared network systems since the telephone allows the caller to know who is receiving the information. With shared networks that are operating correctly, however, anyone with authorized access can obtain the data; if the networks have security flaws, unauthorized persons can obtain the data.

The Administration's National Drug Control Strategy highlights the need to maximize the use and sharing of law enforcement and foreign intelligence information. Exchanging information between law enforcement, DOD, and national foreign intelligence agencies, that have not previously shared information, is particularly challenging. For example, national foreign intelligence agencies collect highly classified information on international drug activities. This information must be sanitized or downgraded before law enforcement agencies can have access to it. Further, there are concerns about protecting sources and methods of gathering information. Misuse of confidential informant information, for example, could be life-threatening.[13]

As part of its master plan, ONDCP and its working groups plan to address the need for security standards across the agencies. However, even if standards are developed, agency officials question whether all the agencies will follow established standards and provide the needed safeguards for maximizing sharing between agencies.

Proliferation of Intelligence Centers Complicates Information Management

As the need for information has grown and more agencies have entered the fight against drugs, more intelligence centers have been created. However, the increased number of centers complicates the management and sharing of counterdrug information. Currently, over 30 centers exist and others are planned. Further, the President's National Drug Control Strategy calls for the establishment of an interagency National Drug Intelligence Center to consolidate information on major drug trafficking

[13]GAO/T-IMTEC-91-6, Mar. 21, 1991.

organizations.[14] Appendix V lists locations of centers in the United States where drug intelligence data are collected and distributed.

As more intelligence centers are formed, coordinating the sharing and use of intelligence between centers has become more of a problem. For example, law enforcement agency officials told us of an instance where information they collected and shared was modified by an intelligence analyst in another agency on the basis of his assumptions rather than on valid information. As a result, an operation to interdict a drug smuggler failed. The growth of intelligence centers also increases the likelihood of duplicate systems being developed, resulting in the inefficient use of resources. For example, in carrying out their statutory detection and monitoring responsibilities, DOD component organizations are building data base systems that, according to some law enforcement officials, basically duplicate systems they already operate. Such a situation occurred as noted in our recent report on DOD's use of its AN/FYQ-93 computers for processing drug-related radar data, where we found that this system duplicates functions being performed by Customs Service systems.[15]

Conclusions and Recommendations

Successful federal action to disrupt the drug trade in the United States depends on the ability of many agencies to collect, process, and exchange information. ONDCP, through its working groups, is collecting data to assess the information needs and capabilities of the drug control agencies, and working toward the development of a master plan to promote necessary agency IRM improvements. Work to correct some voice communications interoperability problems between agencies has already begun.

Notwithstanding this progress, the drug control community faces difficult challenges. In large part, the challenges come from the many agencies involved, all of whom act independently and pursue their own missions. As a result, the agencies have diverse automation capabilities and data needs. Furthermore, IRM weaknesses at the agencies pose barriers to effective drug enforcement. Five issues in particular hurt the community's ability to manage information more efficiently and effectively: (1) there is no central IRM leadership for ensuring information

[14]The February 1991 National Drug Control Strategy Budget Summary reports that the Congress has identified $10 million of DOD's fiscal year 1991 funds for a National Drug Intelligence Center.

[15]Computer Technology: Air Attack Warning System Cannot Process All Radar Track Data (GAO/IMTEC-91-15, May 13, 1991).

management improvements among agencies; (2) some automated information systems are not interoperable; (3) there are no established measures for assuring data integrity with safeguards for protecting individuals' rights; (4) computer system security is not effective in all agencies; and (5) coordinating the sharing and use of drug information is complicated by the growth of intelligence centers that collect, process, and exchange data.

ONDCP plans to begin addressing interoperability, data integrity, security, and aspects of the proliferating sources of intelligence information as part of its overall master plan. This work, however, is far from complete and there is no assurance that the effective and safe exchange of information will occur until these issues are resolved. Moreover, it is not clear how ONDCP intends to address the need for central IRM leadership. Resolving this issue is especially important since ONDCP has to rely on the willingness of scores of agencies to adopt, fund, and carry out those IRM actions necessary to improve information management and sharing across all the drug control agencies.

Therefore, in developing its master plan, we recommend that the Director of ONDCP establish clear, measurable objectives and specific time frames for resolving each of the five issues. In addressing the leadership issue, it is important that ONDCP establish its information system goals, define mechanisms for resolving conflicts that may occur with agencies' primary mission goals, and ensure adequate funding and implementation of drug information programs. We also recommend that the Director report to the appropriate jurisdictional committees within Congress on ONDCP's plans for addressing the five issues and periodically report on the progress made toward resolving them.

As requested by your office, we did not obtain official agency comments on a draft of this report. However, we discussed the information contained in this report with ONDCP and involved agencies and have incorporated their views 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 Director of the Office of National Drug Control Policy, the Director of the Office of Management and Budget, the Secretary of Defense, and the Attorney General. We will also make copies available to the drug control agencies and to others upon request.

This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who may be reached at (202) 275-3455. Major contributors to this report are listed in appendix VI.

Sincerely yours,

Ralph V. Carlone

Ralph V. Carlone
Assistant Comptroller General

Contents

Letter 1

Appendix I Objectives, Scope, and Methodology 18

Appendix II Drug Control Agencies and Counterdrug Activities 20

Appendix III Agencies With Lead Counterdrug Missions 23

Appendix IV Agency Short-Term Automated Data Processing Initiatives 25

Appendix V Counterdrug Intelligence and Operations Centers 29

Appendix VI Major Contributors to This Report 33

Table

Table II.1: Drug Control Agencies With Principal Counterdrug Responsibilities 20

Figure

Figure V.1: Location of Intelligence and Operations Centers 29

Abbreviations

ADNET	Anti-Drug Network
DOD	Department of Defense
EPIC	El Paso Intelligence Center
FinCEN	Financial Crime Enforcement Network
GAO	General Accounting Office
IBIS	Interagency Border Inspection System
IMTEC	Information Management and Technology Division
IRM	Information Resources Management
ONDCP	Office of National Drug Control Policy
TECS II	Treasury Enforcement Communications System II

Objectives, Scope, and Methodology

The Chairman, Subcommittee on Crime and Criminal Justice, House Committee on the Judiciary, requested that we identify automated information systems used by federal agencies in combatting illicit drugs. In April 1991, we provided the Subcommittee with two separate reports—one classified and one For Official Use Only—discussing the results of our counterdrug systems inventory. In subsequent discussions with the Chairman's office, we also agreed to provide the Subcommittee with information on (1) the status of the federal drug control community's efforts to improve counterdrug information management, and (2) issues facing it in this endeavor. This report provides this information. Our work focused on the work of ONDCP as well as other key federal law enforcement, defense, and intelligence agencies fighting to reduce the supply of illegal drugs. We did not review the activities of state and local law enforcement agencies' efforts to improve the management and sharing of drug-related information.

To accomplish these objectives, we interviewed the ONDCP Deputy Director for Supply Reduction and other officials responsible for coordination and oversight of counterdrug information management. Those interviewed included the Chairmen of the Communications Interoperability Working Group and the Automated Data Processing Working Group, as well as agency representatives who participate in the working groups. We also interviewed officials in headquarters offices of the Department of Defense, the Justice Department, the Drug Enforcement Administration, the Customs Service, the Coast Guard, and the Federal Bureau of Investigation.

We visited nine locations to examine the use of automated data processing and communications systems supporting drug interdiction and enforcement at the field level, and to identify problems with exchanging and managing counterdrug information. These locations are generally recognized as the government's key intelligence and operations centers. These centers rely extensively on automated information systems to support their drug interdiction efforts. The centers are operated by the Department of Defense, the Drug Enforcement Administration, the Customs Service, the Coast Guard, and the Department of the Treasury. The locations included the Drug Enforcement Administration's El Paso Intelligence Center; the joint Customs Service and Coast Guard Command, Control, Communications, and Intelligence East and West centers; the Coast Guard's Maritime Intelligence Center and Intelligence Coordination Center; Defense's Joint Task Force Four, Joint Task Force Five, and Joint Task Force Six; and the Department of the Treasury's Financial Crimes Enforcement Network center.

We also collected and reviewed relevant documents, including general background publications about the roles and responsibilities of federal agencies involved in counterdrug efforts, IRM strategic and tactical plans, policy guidance, budget summaries, and ONDCP reports prepared by the Automated Data Processing Working Group and the Communications Interoperability Working Group.

As requested by your office, we did not obtain official comments on a draft of this report. We did, however, discuss the information in this report with ONDCP and agency officials, and have incorporated their comments where appropriate. We performed our work between July 1990 and April 1991. Our work was performed in accordance with generally accepted government auditing standards.

Drug Control Agencies and Counterdrug Activities

Table II.1: Drug Control Agencies With Principal Counterdrug Responsibilities

	Counterdrug activities (see key)					
Organizations	**1**	**2**	**3**	**4**	**5**	**6**
Executive Office of the President						
Office of National Drug Control Policy		X	X		X	X
Department of Justice	X			X		
Bureau of Prisons	X					
Criminal Division	X	X				
Tax Division	X					
Office of U.S. Attorneys	Lead	Lead	X	Lead	Lead	X
Drug Enforcement Administration	Lead	Lead	Lead	Lead	X	X
Federal Bureau of Investigation	Lead	X	X	X	X	X
Immigration and Naturalization Service	X	X	X	X	X	X
U.S. Marshals Service	X	X	X			
Department of the Treasury						
Bureau of Alcohol, Tobacco and Firearms	X	X	X		X	X
Internal Revenue Service	X	X	X			X
U.S. Customs Service	X	X	X	X	Lead	X
Department of Transportation						
Federal Aviation Administration	X		X		X	X
U.S. Coast Guard	X	X	X		Lead	X
Department of State						
Bureau of International Narcotics Matters	X	Lead	X		X	X
Department of Defense (Military)		X	X		X	Lead
Department of Health and Human Services						
Food and Drug Administration				X		
National Institute for Drug Abuse		X		X		

(continued)

Organizations	Counterdrug activities (see key)					
	1	2	3	4	5	6
Intelligence and Other Organizations						
Central Intelligence Agency			X		X	X
Defense Intelligence Agency		X	X		X	X
INTERPOL	X	X	X	X		
National Security Agency		X	X		X	X
Organized Crime Drug Enforcement Task Force	X	Lead	X	Lead	X	X
Operation Alliance					X	X

Key for Counterdrug Activities:
1 Investigation and prosecution
2 International drug control
3 Intelligence
4 Diversion and controlled substances analogue regulation
5 Interdiction and border control
6 Detection and monitoring

Definitions of Counterdrug Activities

Investigation and Prosecution: These actions are designed to destroy drug trafficking infrastructures by incarcerating traffickers, seizing drugs and drug-related assets, and deporting alien traffickers. Successful investigation and prosecution programs reduce drug trafficking and abuse, as well as related crimes such as money laundering, tax evasion, and corruption. Vigorous enforcement delays the supply and distribution of illegal drugs and deters other groups from entering the drug market.

International Drug Control: International drug control seeks to reduce the supply of drugs by helping foreign governments eradicate crops, disrupting and destroying laboratory operations, interdicting drugs close to production sources, arresting and prosecuting major traffickers, and seizing drug-related assets. Drug-demand reduction and public awareness programs in source countries also are important elements of the overall international program.

Intelligence: Intelligence operations are designed to produce, process, and interpret information to meet requirements of the end user. The three categories of drug enforcement intelligence are strategic, tactical, and operational, and they are generally defined as follows: (1) strategic intelligence is information on broad patterns and trends and is used for making high-level policy decisions; (2) tactical intelligence is information

used for specific actions often involving a near-term response such as an arrest or seizure; (3) operational intelligence is information used to support the planning and execution of specific operations, as well as investigations and prosecutions.

Diversion and Controlled Substances Analogue Regulation: This activity focuses on the diversion of licit drugs from legitimate commerce and distribution networks, the diversion of chemicals used in the clandestine production of licit or illicit drugs, and the control of substance analogues that are chemical variants of controlled drugs.

Interdiction and Border Control: Interdiction and border control involves the interception and seizure of illegal drugs entering the United States or traveling through the distribution chain to a user. Interdiction includes intercepting shipments as they move from their departure points in source countries along smuggling routes to United States land, sea, and air borders and within the interior of the country. Three zones are associated with interdiction. They include the departure zone, the transit zone, and the arrival zone. In some cases, the responsibilities of federal agencies involved in interdiction vary depending upon the zone in which the activity occurs. Interdiction also occurs when drugs are intercepted as they are distributed within the interior of the United States.

Detection and Monitoring: These activities, for which DOD is assigned lead responsibility, are generally considered a part of interdiction and border control. The objectives are to detect all aerial and maritime attempts to illegally transport drugs into the country, and to monitor this traffic until it is successfully handed over to law enforcement agencies. As the lead agency, DOD is conducting detection and monitoring operations and coordinating air and sea surveillance by the federal government.

Agencies With Lead Counterdrug Missions

Department of Justice

Executive Office of United States Attorneys

The U.S. Attorneys are the principal litigators for the U.S. government. U.S. Attorneys investigate, prepare, and prosecute federal violations of controlled substances, money laundering, drug trafficking, tax evasion, and violent and organized crime. U.S. Attorneys also oversee the activities of the Organized Crime Drug Enforcement Task Force.

Drug Enforcement Administration

The Drug Enforcement Administration is the lead federal agency for enforcing laws and regulations on narcotics and controlled substances. The agency's primary responsibilities include: investigating major drug violators who operate at interstate and international levels; enforcing regulations governing the legal manufacture and distribution of controlled substances; managing national drug intelligence; and coordinating with federal, state, and local law enforcement agencies and counterparts abroad.

Federal Bureau of Investigation

The Federal Bureau of Investigation investigates violations of criminal drug laws, concurrent with the Drug Enforcement Administration. The mission of the Bureau is to target major multijurisdictional drug trafficking organizations through long-term, sustained investigations. The goals are to dismantle trafficking networks, arrest their leadership, and seize for forfeit their ill-gotten gains. The Bureau participates with the U.S. Attorneys in federal prosecutions and provides assistance to other federal, state, and local law enforcement agencies investigating drug trafficking organizations.

Organized Crime Drug Enforcement Task Force

This program consists of a nationwide structure of 13 regional task forces that use the combined resources and expertise of the program's 11 member federal agencies,[1] in cooperation with state and local investigators and prosecutors, to target and destroy major narcotics-trafficking and money-laundering organizations.

[1] Agency members include: the Drug Enforcement Administration; the Federal Bureau of Investigation; the Immigration and Naturalization Service; the U.S. Marshals Service; the U.S. Customs Service; the Bureau of Alcohol, Tobacco and Firearms; the Internal Revenue Service; the U.S. Coast Guard; the Executive Office of U.S. Attorneys; the Department of Justice Criminal Division; and the Department of Justice Tax Division.

Department of the Treasury

U.S. Customs Service

The Customs Service has responsibility for interdicting illegal narcotics at U.S. ports of entry, and along land, air, and sea borders. The Customs Service also supports the international drug enforcement program.

Department of Transportation

U.S. Coast Guard

The Coast Guard is the lead agency for maritime drug interdiction and has joint responsibility with the Customs Service for air interdiction. The Coast Guard also supports counterdrug intelligence gathering, international operations, and investigations and prosecutions.

Department of State

Bureau of International Narcotics Matters

As the lead agency for coordinating the government's international supply-reduction strategies, the Bureau supports a broad range of drug control programs in foreign countries, focusing on such activities as crop eradication, investigations, interdictions, and intelligence gathering.

Department of Defense

The fiscal year 1989 National Defense Authorization Act assigned DOD the responsibility for serving as the single lead agency for the detection and monitoring of aerial and maritime transit of illegal drugs into the United States. DOD was also charged with integrating into an effective communications network the nation's command, control, communications, and technical intelligence assets dedicated to drug interdiction.

Agency Short-Term Automated Data Processing Initiatives

ONDCP has identified a series of initiatives that it believes will promote improved information management and sharing across drug control agencies. Generally, these efforts include extending the use of automation, expanding existing networks, integrating systems, and modernizing intelligence processing capabilities.

Drug Enforcement Administration and Coast Guard Automation and Automated Data Processing Upgrades at the El Paso Intelligence Center (EPIC)

Reports generated by the Drug Enforcement Administration investigative personnel, a major source of intelligence, are currently available only in paper files, which restricts their utility and availability. The Drug Enforcement Administration is planning a program to automate the production and processing of field reports. In addition, selected portions of the Drug Enforcement Administration's existing, nonautomated data base is being digitized to make it and other data bases amenable to expert system technology and accessible to broad-based analysis.

The Coast Guard also collects and processes vast amounts of information at its Intelligence Coordination Center. However, agency officials told us they rely on manual methods for collecting data. Automated data processing improvements are needed to enhance their processing capabilities and to integrate existing Coast Guard data bases.

EPIC is the counterdrug community's principal tactical intelligence processing and analysis facility.[1] It is dedicated to tactical support of domestic counterdrug operations by state and local, as well as federal law enforcement agencies. It also provides tactical intelligence support to surveillance and interdiction operations against drug shipments into the United States from abroad. EPIC's ability to meet these responsibilities is restricted by the lack of an integrated, adequately sized, automated information handling capability for processing, analyzing, and storing the large quantities of intelligence it receives. According to the National Drug Control Strategy, EPIC is intended to play a major role in the projected expansion of data sharing within the counterdrug community. To meet this need, the Drug Enforcement Administration's plan for upgrading EPIC's automated data processing capabilities is a near-term priority.

[1]Tactical intelligence is defined as information used for specific actions often involving a near-term response such as an arrest or seizure.

Accelerating the Federal Bureau of Investigation's Counterdrug System Development

Developing the Federal Bureau of Investigation's Drug Information System is also considered a high priority. The system, which processes data on organized crime and terrorism, employs artificial intelligence to correlate data from multiple sources, and uses advanced aspects of machine reasoning, graphics, mapping, and visualization. Acceleration of the system's development is needed because the system will be used throughout the counterdrug community as a common medium for data integration and exchange.

Expansion of the Treasury Enforcement Communications System II

The Customs Service's Treasury Enforcement Communications System II (TECS II) is the principal existing common-user network in the law enforcement community. TECS II is accessible both in the United States and at overseas offices. The system provides direct query access to the National Crime Information Center and the National Law Enforcement Telecommunications System, as well as data from the Department of State and the Federal Aviation Administration. TECS II supports up to 9000 users from 16 federal organizations.

Given the criticality of TECS II and its usefulness as a data integration tool, the system's capacity is being expanded to accommodate an increasing work load. The number of connections need to be increased, and existing security features have to be upgraded to adequately protect data derived from various intelligence sources.

The Interagency Border Inspection System (IBIS), which employs TECS II facilities, is a joint Customs, Immigration and Naturalization Service, Agriculture, and State Department system intended to improve the inspection of travellers entering the United States, reduce the need for agencies to operate redundant border control programs, and facilitate the sharing of data through the use of state-of-the-art technologies. IBIS is currently being deployed at international airports in the United States. Proposals to increase the usefulness of the system consist of expanding the IBIS data base to include information from the State Department and other intelligence sources on flagged foreign nationals and extending deployment of the system to other air, land, and maritime ports of entry.

Financial Crime Detection

Detection of financial crimes associated with illegal drugs requires gathering and analyzing voluminous financial data. To assist law enforcement agencies with their money laundering and financial crimes investigations, Treasury created the Financial Crime Enforcement Network (FinCEN) as a full-service data analysis center supporting financial law enforcement. In implementing FinCEN, Treasury has created a number of initiatives related to automated data processing that include developing a FinCEN information handling capability, providing communications links to other data centers and systems, and expanding Internal Revenue Service systems to help process financial reports.

Department of Defense

Detection and Monitoring

The fiscal year 1989 National Defense Authorization Act assigned several responsibilities to the Secretary of Defense, including requirements that the Department (1) serve as the single lead agency of the federal government for the detection and monitoring of aerial and maritime transit of illegal drugs into the U.S. and, (2) integrate U.S. command, control, communications, and technical intelligence assets dedicated to drug interdiction into an effective communications network.

In support of both objectives, Defense's Joint Chiefs of Staff implemented the Anti-Drug Network (ADNET) to provide a medium for tactical intercommunications and data exchange among the diverse drug control agencies that participate in interdictions. ADNET consists of: a message distribution system to provide common access to fused counterdrug data; a Joint Visually Integrated Display System to provide timely detection and monitoring information to all operational levels; and graphic overlays to highlight weather, areas of responsibility, and geographic data. ADNET provides a communications link between the three Defense Joint Task Force centers: the joint Customs Service and Coast Guard Command, Control, Communications, and Intelligence center in Miami, Florida; the Customs Service Command, Control, Communications, and Intelligence center in Riverside, California; and EPIC in El Paso, Texas.

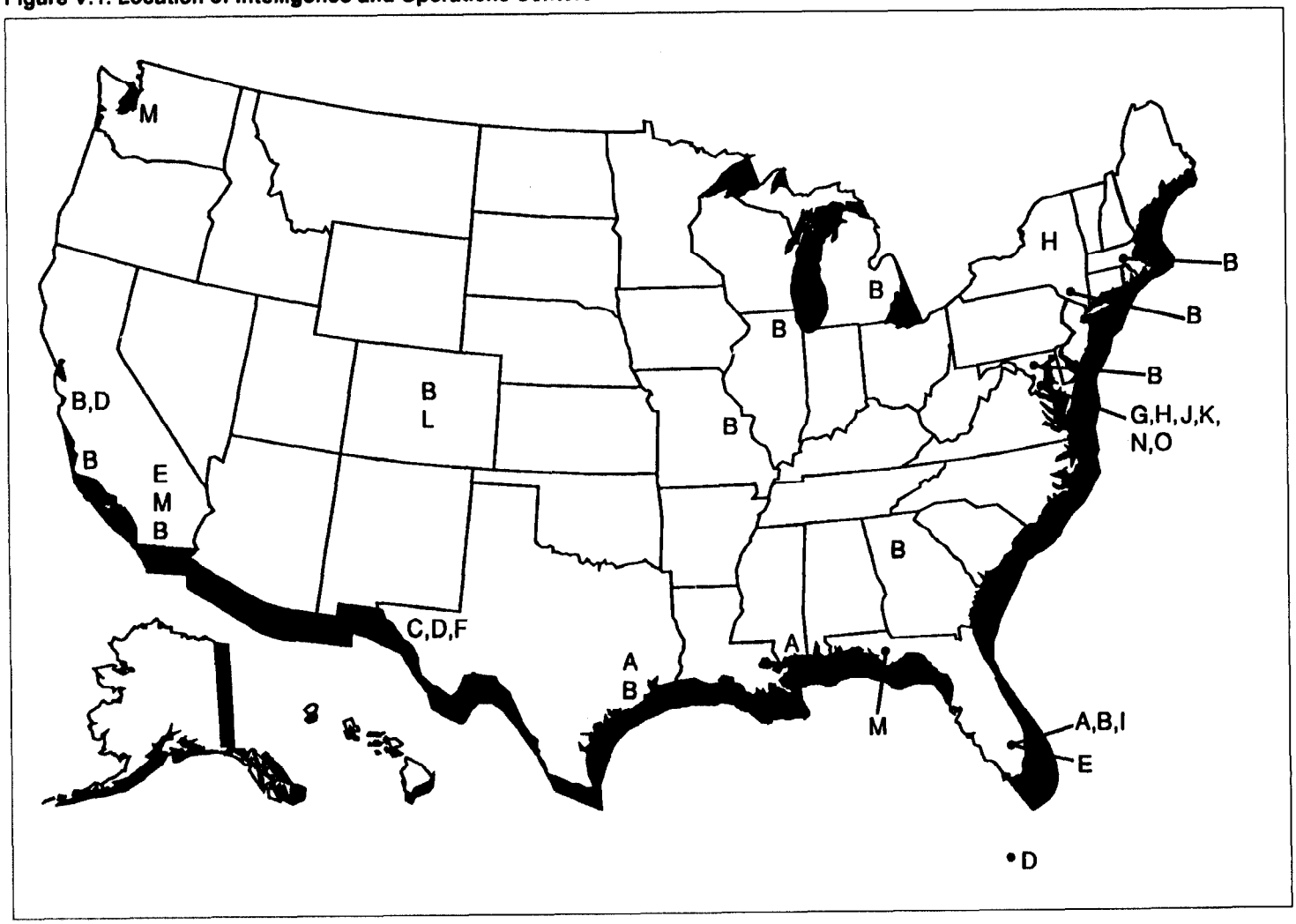
Expanded Sharing of National Foreign Intelligence Program Information

The Joint Maritime Information Element is a product of a broad consortium of drug control agencies. It consists of a centralized data base of

maritime activities worldwide, including both dynamic ship-movement data and extensive reference files. The system is currently being deployed to provide remote access to staff working on interdictions at key U.S. maritime ports of entry.

Counterdrug Intelligence and Operations Centers

Figure V.1: Location of Intelligence and Operations Centers



A - Blue Lightning Operations Center
B - Organized Crime Drug Enforcement Task Force
C - Operation Alliance
D - Joint Task Forces
E - Command, Control, Communications, and Intelligence
F - El Paso Intelligence Center
G - Financial Crime Enforcement Network
H - Intelligence Coordination Center
I - Maritime Intelligence Center
J - Counternarcotics Center
K - Joint Tactical Intelligence Center and National Military Intelligence Center
L - North American Aerospace Defense Command Tactical Intelligence Cell
M - Sector Operational Control Center
N - Drug Enforcement Administration Office of Intelligence
O - Federal Bureau of Investigation Drug Intelligence Unit

Blue Lightning Operations Centers

Operated by the Customs Service and the Coast Guard, these three operations and intelligence centers use radar data and intelligence information to coordinate maritime interdictions along the southeast coast of the United States. The centers are located in Houston, Texas; Gulfport, Mississippi; and Richmond Heights, Florida.

Organized Crime Drug Enforcement Task Force

The Organized Crime Drug Enforcement Task Force is a major federal cooperative program for narcotics investigations and prosecutions that specifically targets major drug trafficking organizations. The task force initiative was started in 1983 and serves the counterdrug community by coordinating federal agencies' attacks on drug trafficking and organized crime. Thirteen regional task forces are located in major cities throughout the country.

Operation Alliance

This operation is a joint counterdrug program initiated in 1986 to coordinate surveillance and interdiction along the U.S. southwest border. Operation Alliance includes representatives from the Immigration and Naturalization Service, the Border Patrol, the Customs Service, the Drug Enforcement Administration, and the Internal Revenue Service. Other federal, state, and local agencies participate as required. Multiagency operations that Operation Alliance coordinates are directed from its location in El Paso, Texas.

Joint Task Forces

Defense performs its counterdrug detection and monitoring activities through various field commands. The commands perform intelligence collection, analysis, and dissemination in support of Defense and law enforcement agency operations within their areas of responsibility. To assist in this work, the U.S. Atlantic Command, the U.S. Pacific Command, and the U.S. Forces Command established three respective Joint Task Force centers. The U.S. Atlantic Command's Joint Task Force Four, located in Key West, Florida, and the U.S. Pacific Command's Joint Task Force Five, located in Alameda, California, serve as focal points for detection and monitoring on the East and West coasts. The U.S. Forces Command's Joint Task Force Six, located in El Paso, Texas, coordinates all Defense support to law enforcement agencies along the southwest border.

Command, Control, Communications, and Intelligence Centers

The Customs Service and the Coast Guard operate Command, Control,

Communications, and Intelligence centers that monitor air traffic to identify suspected drug smuggling, assist federal agencies in gathering tactical intelligence, and coordinate air interdictions within specific areas of responsibility. The Command, Control, Communications, and Intelligence West Center in Riverside, California, operated by the Customs Service, monitors air traffic in the Southwest and on the Pacific Coast. The Command, Control, Communications, and Intelligence East Center in Richmond Heights, Florida, operated jointly by the Customs Service and the Coast Guard, monitors air traffic on the East and Gulf Coasts.

El Paso Intelligence Center

EPIC is a Drug Enforcement Administration-led, multiagency center established in 1974 as a cooperative effort to collect, process, and disseminate information on illicit drug trafficking and other activities of interest to law enforcement organizations, including smuggling of illegal aliens and weapons trafficking. EPIC is the government's principal tactical drug intelligence and interdiction center.

Financial Crime Enforcement Network

FinCEN was established in 1990 by the Treasury as a full-service data analysis center located in Washington, D.C. The objective of the center is to support financial law enforcement by collecting and analyzing information on financial activities of individuals and organizations that may reveal illegal actions, including those associated with illegal drug trafficking.

Intelligence Coordination Center

Located at Coast Guard headquarters in Washington, D.C., the Intelligence Coordination Center coordinates drug intelligence gathering. The center provides Coast Guard field units with strategic intelligence by collecting and analyzing counterdrug data from other agencies.

Maritime Intelligence Center

The Seventh Coast Guard District operates the Maritime Intelligence Center in Miami, Florida. The center collects, collates, analyzes, and disseminates tactical intelligence for the purpose of interdicting suspect vessels in the Caribbean.

Counternarcotics Center

The Counternarcotics Center was established in 1989 to provide overall guidance and support to the intelligence community's counterdrug

effort.[1] The center provides an interface between national intelligence producers and consumers for the benefit of the counterdrug community.

Joint Tactical Intelligence Center and National Military Intelligence Center

Operated by the Defense Intelligence Agency, the Joint Tactical Intelligence Center conducts analyses and provides strategic and operational information for foreign interdiction and drug eradication operations. The Defense Intelligence Agency's National Military Intelligence Center facilitates coordination of counterdrug intelligence collection and distribution.

Tactical Intelligence Cell and Sector Operational Control Centers

Defense's North American Aerospace Defense Command does not have a Joint Task Force. Its intelligence functions are conducted mainly by its Tactical Intelligence Cell. In addition, it has regular small intelligence staffs at its Sector Operational Control Centers that perform limited counterdrug functions such as monitoring air traffic and passing information on suspects to local commands and law enforcement agencies.

The Drug Enforcement Administration's Office of Intelligence

The Office of Intelligence, which is based in Washington D.C., provides direct analytical support to the Drug Enforcement Administration's enforcement operations. While information from other agencies is reviewed, the principal focus of these analyses is the Drug Enforcement Administration's information and investigative needs.

The Federal Bureau of Investigation's Drug Intelligence Unit

The Drug Intelligence Unit, which is based in Washington D.C., provides direct analytical support to the Bureau's investigative efforts. These efforts are directed against operations of major drug trafficking organizations. The principal focus of the unit's activities surrounds the analyses of information generated by and for the Bureau's investigations.

[1]Principal agencies included in the intelligence community are the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, Federal Bureau of Investigation, and intelligence organizations of the State Department and each military service.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.

Steven A. Schwartz, Assistant Director
William D. Hadesty, Technical Assistant Director
Mark D. Shaw, Evaluator-in-Charge
B. Gail Moore, Staff Evaluator
Keith Landrum, Staff Evaluator
Kevin G. McCarthy, Staff Evaluator
Mary T. Marshall, Reports Analyst

Office of the General Counsel

Richard Seldin, Senior Attorney

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

Ordering Information

The first five copies of each GAO report are 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.