



governmentattic.org

"Rummaging in the government's attic"

Description of document: **Department of Justice (DOJ) Office of the Inspector General (OIG) Audit Division, Audit Report 05-25: The Drug Enforcement Administration's Payments to Confidential Sources to the Drug Enforcement Administration (DEA), May 2005**

Requested date: 04-March-2006

Released date: 26-July-2010

Posted date: 23-August-2010

Source of document: FOIA Request
Office of the Inspector General
Office of General Counsel
950 Pennsylvania Ave., N.W.
Room 4726
Washington, D.C. 20530
Fax: 202-616-9152

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



U.S. Department of Justice

Office of the Inspector General

July 26, 2010

Subject: Freedom of Information/Privacy Act Request (FOIA) [06-OIG-107]

I am writing in response to your March 4, 2006 request seeking audit reports produced by the Office of the Inspector General.

Enclosed please find one audit report responsive to your request. With regard to OIG report titled "The Drug Enforcement Administration's Payments to Confidential Sources to the Drug Enforcement Administration (DEA)", after consulting with the DEA, it has been determined that portions of this report are exempt from FOIA release pursuant to 5 U.S.C. §552(b)(7)(C),(D), and (E).

With regard to the remaining requested audit reports, the OIG is continuing to consult with other components regarding the releasability of the reports. We will inform you when we reach a final determination regarding those reports.

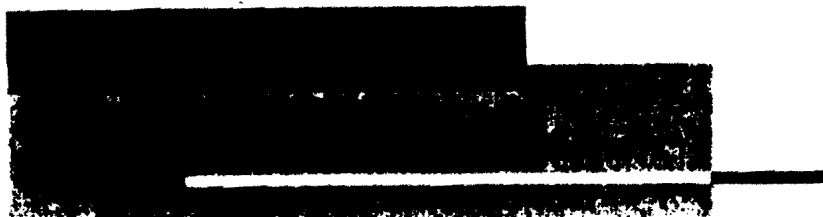
If you are dissatisfied with my action on this request, you may appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530. Your appeal must be received by OIP within 60 days of the date of this letter. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." In the event you are dissatisfied with the results of any such appeal, judicial review will thereafter be available to you in the United States District Court for the judicial district in which you reside or have your principal place of business, or in the District of Columbia, which is also where the records you seek are located.

Sincerely,

A handwritten signature in blue ink, reading "Deborah M. Waller", is positioned above the printed name.

Deborah Marie Waller
FOI/PA Specialist
Office of the General Counsel

**LIMITED OFFICIAL USE -
NOT FOR PUBLIC RELEASE**



**THE DRUG ENFORCEMENT
ADMINISTRATION'S
PAYMENTS TO CONFIDENTIAL
SOURCES**

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 05-25
May 2005

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE
This document contains information that is exempt from public release under the Freedom of Information Act, 5 U.S.C. 552, because its disclosure could result in the identification of confidential sources or other improper disclosure of the information contained herein.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

THE DRUG ENFORCEMENT ADMINISTRATION'S PAYMENTS TO CONFIDENTIAL SOURCES

EXECUTIVE SUMMARY

The Confidential Source program is an important tool used by the Drug Enforcement Administration (DEA).¹ DEA officials state that without confidential sources, the DEA could not effectively enforce the controlled substances laws of the United States. Confidential sources come from all walks of life and are significant to initiating investigations and providing information or services to facilitate arrests and seizures of drugs and cash. According to the DEA, it has approximately 4,000 active confidential sources at any one time, and more than 113,000 have been in an activated status at some point in time since 1996. In comparison, the DEA had over 5,000 authorized special agents in Fiscal Year (FY) 2004. Payments to confidential sources represent a small percentage (about 2 percent) of the DEA's total budget.

Although confidential sources can be critical to an investigation, special care must be taken to carefully evaluate and closely supervise their use. Confidential sources are motivated by many factors, including fear, financial gain, avoidance of punishment, competition, and revenge; therefore, the credibility of a source must be balanced against the information they provide. Widely publicized cases of informants gone awry, such as [REDACTED] with the Federal Bureau of Investigation (FBI) and [REDACTED] with the DEA, highlight the need for special care in dealing with confidential sources.² The [REDACTED] case in particular provided the impetus for the development of the Attorney General Guidelines Regarding the Use of

B(7)(D)(C)

¹ The Attorney General Guidelines Regarding the Use of Confidential Informants uses the term "Confidential Informant," while the DEA uses the term "Confidential Source." Both terms refer to any individual who provides useful and credible information to a Department of Justice (DOJ) law enforcement agent regarding criminal activities, and from whom the DOJ law enforcement agent expects or intends to obtain additional useful and credible information regarding such activities in the future. For consistency throughout this report we use the term "Confidential Source."

B(7)(C)(D)

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Confidential Informants (Attorney General Guidelines), with which all Justice law enforcement agents are required to comply.³

Confidential sources can present significant challenges to a law enforcement agency. As the DEA acknowledged, confidential sources are generally not "choir boys," and the DEA must interact and rely on information from confidential sources whose credibility may be questionable. Consequently, their use must be balanced against the value of the information provided.

From FY 1998 - 2002, the DEA paid confidential sources approximately \$30 - \$35 million per year. As shown in the following table, the payments are categorized as [REDACTED] B(7)(E)

D(7)(E) **DEA Payments to Confidential Sources⁵**

Fiscal Year	[REDACTED]						Total
1998	\$18,237,343	2,388,367	983,921	118,395	4,671,145	8,319,755	\$34,718,926
1999	\$16,970,922	3,915,395	325,650	39,794	3,839,098	5,919,895	\$31,010,754
2000	\$19,271,253	2,494,013	255,189	65,748	4,143,734	6,604,120	\$32,834,057
2001	\$19,142,035	2,507,827	2,416,340	88,698	6,000,596	4,920,638	\$35,076,134
2002	\$19,019,444	2,993,265	1,949,574	52,193	3,415,916	4,652,032	\$32,082,424

Source: DEA Federal Financial System June 2003

The Office of the Inspector General (OIG) initiated this audit to assess the DEA's compliance with regulations concerning individuals who provide information for payment, and the DEA's controls over confidential source payments.⁶ To conduct our audit, we researched the DEA's Confidential Source Program by reviewing pertinent documents, including the four

³ The Attorney General Guidelines were issued in January 2001 and revised in May 2002. See Appendix VIII for the Attorney General Guidelines.

⁴ Appendix VI lists the definitions for the types of confidential source payments.

⁵ As discussed in Finding II, the DEA does not maintain an effective system for determining payments to confidential sources. Therefore, the dollar amounts supplied by the DEA may not accurately reflect the total amounts paid to confidential sources.

⁶ See Appendix I for more information on this audit's objectives, scope, and methodology.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

versions of the DEA Agent Manual in effect since 1998; the DEA Financial Handbook, undated (obtained from the DEA in May 2003); and the Attorney General Guidelines dated January 8, 2001, and May 30, 2002. We reviewed the DEA's process of establishing, paying, and monitoring confidential sources by reviewing 150 confidential source files, and considered the impact of utilizing the confidential source by reviewing 64 closed Investigative case files. We also conducted interviews of DEA agents and finance personnel in headquarters and seven Division offices. We performed our fieldwork at DEA Headquarters in Arlington, Virginia, and the Washington, New York, Miami, Los Angeles, Phoenix, Houston, and Chicago Division offices.

FINDINGS

The DEA Can Improve Risk Management Over the Use of Confidential Sources

The risks surrounding the use of confidential sources challenge the DEA to ensure that sources are not only credible, but also that agents do not develop close financial or personal relationships with sources that could compromise a case. Managing confidential sources requires the DEA to constantly assess the risk for each source it utilizes. In this context, risk assessment is the continual identification and analysis of relevant adverse factors that are weighed against the potential benefit of using the confidential source. Although the DEA adopted policies and procedures to manage the risk of using confidential sources, we found that the DEA can improve its risk management in the following areas: 1) initial suitability reporting and recommendations, 2) categorization of confidential sources, 3) continuing suitability reporting and recommendations, 4) review of long-term confidential sources, and 5) maintenance of impeachment information.

Initial Suitability Reporting and Recommendations

The Attorney General Guidelines outline requirements that the DEA must fulfill before activating a confidential source. Specifically, case agents for confidential sources need to complete and sign a written Initial Suitability Report and Recommendation that addresses specific risk factors, or indicate on the report that a particular factor is not applicable.⁷ According to the DEA Agent Manual, although a suitability statement need not consist of more than one paragraph, it must detail the specific benefits of utilizing the source

⁷ Examples of suitability factors are criminal background and prior record as a witness. For a complete listing of suitability factors, see Appendix IV.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

and provide the reasons for utilizing a source despite any adverse information.

We tested 150 confidential source files to determine if written initial suitability risk assessments were completed. Of the 150 files reviewed, 63 confidential sources were activated after the January 2001 effective date of the Attorney General Guidelines. Our testing revealed that only 28 of 150 confidential source files (19 percent) contained written initial suitability assessments addressing the specific risk assessment factors. Further, only 10 of the 63 confidential source files (16 percent) activated after January 2001 requirement contained written initial suitability assessments addressing the specific risk assessment factors. Of the three division offices we first visited, we found that written initial suitability risk assessments generally were completed in the Washington, D.C., and New York offices, but not in the Miami office. We subsequently expanded our testing in the Los Angeles, Phoenix, Houston, and Chicago offices (110 of the 150 confidential source files reviewed) to determine if the suitability factors were addressed in documents other than a formal risk assessment.

We found that biographic information such as age, alien status, and contact information was generally included on the Confidential Source Establishment Forms (DEA 512). However, information regarding other suitability factors was not readily apparent on that form. That information was sometimes found on a variety of documents, including the Reports of Investigation Form (DEA 6). During our audit, we had to review the entire confidential source file in order to determine whether some of the suitability factors had been addressed. This same time-consuming file review process has to be used by agents and supervisors who were not present when the confidential source was established so that they are aware of the information relevant to the suitability factors.

The majority of DEA 512's we reviewed had general statements indicating, in essence, that the benefits of using the confidential source outweighed the risks, without specifying either the benefits or the risks. These descriptions do not meet the requirements of the DEA Agent Manual or the Attorney General Guidelines that suitability statements detail the specific benefits of utilizing the confidential source despite the identified risk factors.

Moreover, DEA training information supplied to the OIG by the DEA Confidential Source Unit stated that written risk assessments of potential confidential sources were not required and were to be performed at the discretion of the Special Agent in Charge. In fact, the Los Angeles office had a formal divisional order that stated agents were not to write risk

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

assessments, and the New York office also issued guidance that stated a separate written risk assessment was no longer necessary. The Miami Special Agent in Charge waived the requirement to document risk assessments. The fact that DEA does not require a written suitability report that addresses all the specific factors means the DEA Agent Manual is not in compliance with the Attorney General Guidelines.

We believe that a written, comprehensive initial suitability risk assessment is critical to measuring the benefits of utilizing a confidential source, and it could help other agents who want to use the confidential source but may be unaware of pertinent derogatory information concerning the source. In addition, this risk assessment should guide the nature and extent of confidential source monitoring.

Categorization of Confidential Sources

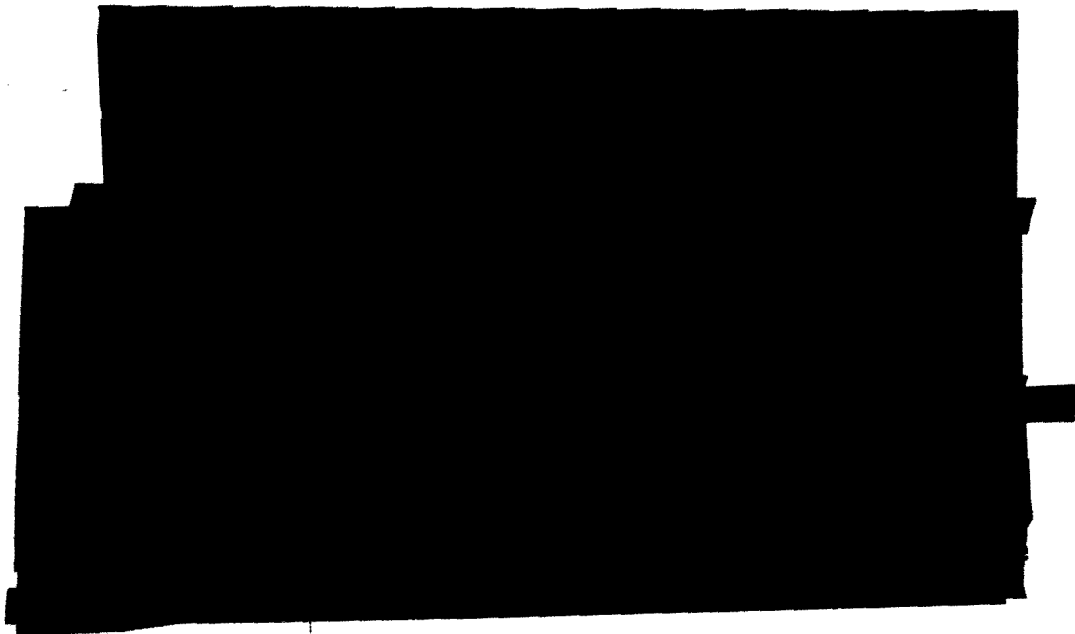
[REDACTED]

B(7)(C)

[REDACTED]

* See Appendix III for a description of the DEA categories of confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE



B(7)(E)

Continuing Suitability Reporting and Recommendation

Once a confidential source has been established, the Attorney General Guidelines require the case agent to review, at least annually, the confidential source's file and complete and sign a written Continuing Suitability Report and Recommendation which must be forwarded to a field manager for written approval. The purpose of the Continuing Suitability Report and Recommendation is to determine whether the risk of using a source has changed since the initial evaluation, and whether the confidential source should continue to be utilized. In completing the Continuing Suitability Report and Recommendation, the case agent must address the same factors outlined in the initial suitability determination (or indicate that a particular factor is not applicable), the length of time that the individual has been registered as a confidential source, and the length of time the source was handled by the same agent.

Instead of an annual review, the DEA requires first-line supervisors and controlling agents to perform Quarterly Management Reviews of Confidential Source Utilization (Quarterly Management Review) on each active confidential source. Our review of 150 confidential source files revealed that none of the Quarterly Management Reviews addressed all continuing suitability factors outlined in the Attorney General Guidelines. Although some of the factors were addressed, most reviews contained

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

generic or boilerplate statements such as "no changes in biographic information." Given that the initial suitability report is generally not written and therefore does not provide information on all suitability factors, the lack of specific information in the Quarterly Management Reviews makes it even more difficult to determine if agents are aware of the risks of using the source, and are taking these risks into consideration when determining if the confidential source is suitable and the extent that they should be monitored.

Review of Long-Term Confidential Sources

One of the purposes of the Attorney General Guidelines is to provide more oversight of agents handling confidential sources by having individuals who are not as close to confidential sources make critical decisions over payments and other matters. The Attorney General Guidelines require a "Confidential Informant Review Committee" to review confidential sources that have been active for more than six consecutive years, and to the extent such a confidential source remains active, every six years thereafter. The DEA implemented this process through its Sensitive Activity Review Committee. This Committee convenes not only to review long-term confidential sources, but also for a number of other reasons, including conferences involving property, money laundering, and proprietary storefront operations.

When we spoke to the Undercover and Sensitive Operations Unit Chief, he stated that prior to November 2003 the Committee had not reviewed any matters relative to DEA long-term Confidential Sources. He also stated that the Committee does not review confidential source files. Instead, the committee reviews an Excel Spreadsheet that contains the names and other information about long-term confidential sources. During the review, the Confidential Source Unit Section Chief is available to answer questions that arise that cannot be explained by the information contained in the spreadsheet. Although a committee member may review a confidential source file, the Unit Chief stated that he does not believe this is necessary. The Unit Chief also stated the Committee is unlikely to question the judgment of a Special Agent in Charge who already has reviewed the information in the confidential source file.

Further, the DEA has no rating system to assess the quality of the information provided or services rendered by confidential sources. Instead, it relies on an agent's knowledge and skill to assess whether a confidential source is effective.

We believe the DEA should strengthen its management over long-term confidential sources. We believe the Sensitive Activity Review

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Committee relies too heavily on the Headquarters Confidential Source Unit and Special Agents In Charge because the DEA does not adequately document required suitability factors in its initial suitability report and its quarterly management reviews. In our view, the Sensitive Activity Review Committee should provide a high level, independent review of long-term confidential sources. If the committee relies solely on the Special Agents In Charge and the Headquarters Confidential Source Unit without independently reviewing pertinent original information itself, the value of its oversight is significantly diminished.

Maintenance of DEA Impeachment Information

The DEA Agent Manual requires agents to provide prosecutors with all discoverable information pertaining to any confidential source who may be utilized as a witness. This information includes payments to the confidential source, any oral or written agreements between the DEA and the confidential source, and any impeachment information known by the DEA that may affect the credibility of the confidential source. Examples of impeachment information are a confidential source's criminal record, a substance abuse problem, or instances where the confidential source has given false testimony or statements.

The DEA relies on agents to perform manual searches of the confidential source files in order to report discovery information. As noted earlier in this report, the DEA does not detail by factor the confidential source's suitability either when initially establishing the source or during the quarterly review. Therefore, it may be difficult for an agent who was not present at either the establishment or quarterly briefing of a confidential source to discover impeachment information. We believe the DEA can improve its tracking of impeachment information by adding a module to its Confidential Source System (CSS).⁹

The DEA Lacks an Effective and Accurate Confidential Source Payment System

The DEA is required by the Attorney General Guidelines to establish accounting and reconciliation procedures that reflect *all* monies paid to confidential sources. The primary systems utilized by the DEA to process

⁹ The DEA Confidential Source System is an automated, limited-access database containing a record of all confidential sources assigned a unique number.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

and account for confidential source payments are the Federal Financial System and the CSS Dollar database.¹⁰

Our audit identified deficiencies in the DEA's accounting and reconciliation of confidential source payments that led us to conclude that the DEA does not have an effective confidential source payment tracking system. Specifically, we found inconsistencies in the amounts and types of payments paid to confidential sources, deficiencies with the accounting and monitoring of calendar year and lifetime payments, problems with the systems used to account for confidential source payments, and control breakdowns that indicate closer supervisory oversight of confidential source payments is needed.

Discrepancies in the Amounts and Types of Payments to Confidential Sources

As part of our review to assess how the DEA accumulates confidential source payment information, we asked the DEA's Office of Finance to provide us with the total amount of confidential source payments from FY 1998 through FY 2002 by budget category. The DEA's Office of Finance queried the Federal Financial System in July 2002 and June 2003 and provided us with different payment amounts regarding the same time period. Our review of the payments revealed significant discrepancies in the amounts and types of payments provided to confidential sources as shown in the following table.

¹⁰ The Federal Financial System is a Department of Agriculture system that handles the DEA financial information on a contract basis. The DEA utilizes the Federal Financial System to process confidential source payments. The CSS Dollar database is a subsystem of the DEA's Confidential Source System, and is the electronic record-keeping system for monies paid to confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

**Comparison of Historical
Confidential Source Payment Information**

Types of Confidential Source Payments

FY 1998:						
July 2002	\$17,932,802	\$0	\$976,322	\$97,719	\$4,676,145	\$8,291,265
June 2003	\$18,237,343	\$2,388,367	\$983,921	\$118,395	\$4,671,145	\$8,319,755
Discrepancy	\$304,541	\$2,388,367	\$7,599	\$20,676	\$5,000	\$28,490
FY 1999:						
July 2002	\$16,885,001	\$0	\$325,647	\$39,839	\$3,901,098	\$5,891,315
June 2003	\$16,970,922	\$3,915,395	\$325,650	\$39,794	\$3,839,098	\$5,919,895
Discrepancy	\$85,921	\$3,915,395	\$3	\$45	\$62,000	\$28,580
FY 2000:						
July 2002	\$19,110,333	\$0	\$250,408	\$65,248	\$4,134,434	\$6,514,120
June 2003	\$19,271,253	\$2,494,013	\$255,189	\$65,748	\$4,143,734	\$6,604,120
Discrepancy	\$160,920	\$2,494,013	\$4,781	\$500	\$9,300	\$90,000
FY 2001:¹³						
July 2002	\$19,006,761	\$0	\$2,409,769	\$88,697	\$5,986,800	\$4,828,738
June 2003	\$19,142,035	\$2,507,827	\$2,416,340	\$88,698	\$6,000,596	\$4,920,638
Discrepancy	\$135,274	\$2,507,827	\$6,571	\$1	\$13,796	\$91,900

Source: DEA Federal Financial System. The payment information was supplied in July 2002 and June 2003 regarding the same time period. The amounts do not include payments DEA made using non-appropriated funds such as High Intensity Drug Trafficking Areas (HIDTA).

When we asked the DEA about the discrepancies, we were informed by the audit liaison that:

¹¹ See Appendix VI for a description of the Budget Object Codes used to pay confidential sources.

[REDACTED]

¹³ In April 2003, the DEA Office of Finance provided detailed transactions regarding FY 2001 confidential source payments. The total of the detailed transactions for FY 2001 was \$11 million less than the total amount supplied in July 2002 and \$14 million less than the total amount supplied in June 2003.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

B(7)(E)

B(7)(E)

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The query run for the OIG by the Office of Finance was run out of the Federal Financial System, as was the query provided at the [audit] entrance conference. Because errors in the Federal Financial System may be made at any time and reconciliations completed quarterly, the DEA can confirm that numbers are correct only as of the day they are run. The DEA cannot certify that these same numbers would result from a query conducted on the day the [OIG] report is issued. The DEA is willing to re-run the query closer to the report publication date, but can only confirm those numbers as of the date the query is run.

We are concerned by the DEA's response because historical financial data should not significantly change over time. Significant changes to historical data years after the close of a fiscal year calls into question the reliability of the data and the system.



The Section Chief for the Confidential Source Unit did not have an explanation as to why the Office of Finance treated these transactions differently than other Confidential Source payments. However, the fact that the Office of Finance does not consider payments to foreign officials as confidential source payments explains why these payments were not included in the July 2002 listing of confidential source payments. We believe the DEA must resolve this inconsistency between the Confidential Source Unit and the Office of Finance and determine if payments using budget object code 2533 are confidential source payments or not. Otherwise, the DEA will not have complete assurance that it is fully accounting for all confidential source payments as required by the Attorney General Guidelines.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Accounting and Monitoring of Annual and Aggregate Payments

The Attorney General Guidelines state that payments to a confidential source that exceed an aggregate of \$100,000 within a one-year period shall be made only with the authorization of a senior field manager and the express approval of a designated senior headquarters official. In addition, regardless of the time frame, any payments to a confidential source that exceed an aggregate of \$200,000 should be made only with the authorization of a senior field manager and the express approval of a designated senior headquarters official. During our audit of 150 confidential source files and 64 case files, we noted a total of 176 different confidential sources. We requested the DEA to provide us with the lifetime payments for these 176 confidential sources. We determined that 27 of these 176 (15.3 percent) had received lifetime payments totaling more than \$200,000. Further, we observed 10 of the 176 (5.6 percent) confidential sources had payments totaling greater than \$1 million. However, our audit revealed weaknesses with how the DEA monitors calendar year and lifetime payments and accounts for non-appropriated funds. Without reviewing the confidential source files in every office that utilized these confidential sources, we could not determine if the appropriate approvals were obtained.

Accounting for Non-Appropriated Funds. The DEA Agent Manual states that only DEA-appropriated funds will be included in the determination of calendar year and lifetime payment amounts, while the Attorney General Guidelines do not distinguish between appropriated and non-appropriated funds. The DEA Agent Manual goes on to say that all confidential source payments using appropriated funds or funds from other agencies must be documented on the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103). However, payments using non-appropriated funds - such as High Intensity Drug Trafficking Area (HIDTA) funds - are not processed through the Federal Financial System and consequently are not included in the CSS Doliar database of payments.¹⁴ This means that the DEA does not consider payments using non-appropriated funds in determining whether payments to a confidential source exceed calendar year or lifetime payment caps. Further, since the confidential source payments using HIDTA funds are not processed through the Federal Financial System, the DEA could not provide the OIG with the total confidential source payments using HIDTA funds.

¹⁴ According to the Office of National Drug Control Policy, the mission of the HIDTA program is to enhance and coordinate drug-control efforts among local, state, and federal law enforcement agencies in order to eliminate or reduce drug trafficking and its harmful consequences in critical regions of the United States. The mission includes coordination efforts to reduce the production, manufacturing, distribution, transportation, and chronic use of illegal drugs, as well as attendant money laundering of drug proceeds.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Monitoring Calendar Year and Lifetime Payments. In addition to not counting non-appropriated funds towards the calendar year and lifetime payments, we noted other problems with how the DEA monitors annual (calendar year) and aggregate (lifetime) payments. During our audit, DEA officials first stated that the CSS Dollar database monitors the annual and lifetime payments and "flags" payments that put the totals over the limits. The flag is supposed to signal that headquarters approval is required to exceed the cap; however, it does not prevent the payment.

In addition, we were informed by both the former and current Section Chief of the Confidential Source Unit, numerous DEA agents, and five of the seven Confidential Source Coordinators for the offices we reviewed that the CSS Dollar database is unreliable. The Section Chief for the Confidential Source Unit provided a series of e-mails that outlined long-standing problems the DEA has experienced in populating the CSS Dollar database.¹⁵ The e-mails indicated time lags in processing the payments, a lack of quality controls, and a communication disconnect between the DEA Office of Finance and the Confidential Source Unit regarding who is responsible for the CSS Dollar database and correcting the problems. The Section Chief for the Confidential Source Unit said that incomplete records in the data supplied to the CSS Dollar database (incorrect date, case number, and office identifier) make it impossible to perform a proper audit of a confidential source's payment history.

Later during the audit, the DEA stated that Confidential Source Coordinators monitor the calendar year and lifetime payments by manually adding up the payments listed in the confidential source files. Yet, confidential sources could be active in more than one office, so confidential source coordinators must contact all offices in which the source is active to arrive at a source's total calendar and lifetime payments.

To determine if the DEA is monitoring calendar year and lifetime caps apart from using the CSS Dollar database, we reviewed documentation in the confidential source files for evidence of cap monitoring. During our review of 150 confidential source files, we noted that caps were only sporadically documented on Quarterly Management Reviews, Receipts for Cash or Other Items (DEA 12), and Confidential Source Establishment (DEA 512). Although we noted a few memoranda requesting cap increases, we did not find any formal process or consistent practice used by the DEA to monitor calendar year and lifetime payments. We also did not identify any

¹⁵ These long-standing weaknesses identified in the e-mails also contributed to the DEA's problems of determining the amounts paid to confidential source Andrew Chambers.

LIMITED OFFICIAL USE – NOT FOR PUBLIC RELEASE

formal reconciliation of the CSS Dollar database, the Federal Financial System, and the confidential source payment records.

Because the CSS Dollar database is unreliable and the DEA does not have a formal or consistent practice to monitor calendar or lifetime payments, we were unable to determine if confidential source payment levels were exceeded without the appropriate approvals or verify that the DEA was effectively monitoring payments.

Problems with the Federal Financial System and the CSS Dollar Database

During our audit, we noted problems with the processing of confidential source payments in the Federal Financial System, the lack of audit trails, and delays in processing confidential source payments.

Issues with the Federal Financial System Vendor Name, Case Tables, and the Correction of Errors. In order to enter confidential source payments into the Federal Financial System, the DEA requires a "vendor name."¹⁶ During our audit, the DEA Office of Finance queried the Federal Financial System for FY 2002 and found 79 records where the Budget Object Code was 2530 (Securing of Information), but the vendor name was not a confidential source. In February 2004, the DEA made enhancements to the Federal Financial System to ensure that confidential source budget object codes matched a confidential source. While the enhancement better validates vendor names, a problem still exists with the validation system. Specifically, if a confidential source is deactivated, the vendor name *is not* deactivated; therefore, a payment could be processed with a deactivated confidential source vendor name. When we discussed this issue with the DEA, we were told that the Confidential Source Coordinator would catch this problem when the copy of the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103) was filed in the confidential source file. However, even if the Confidential Source Coordinator noted this error when the paperwork is filed, the funds would have already been paid. Consequently we believe the DEA should further enhance the controls over confidential source payments to prevent a deactivated confidential source from being used to obligate or expend funds. This can be done by removing deactivated confidential source vendor names from the validation table.

Another improvement made by the DEA in February 2004 was the validation of the case number field in the Federal Financial System. Previously, only the first five digits of the case number were validated and the remaining four digits could be any combination of numbers up to 9999.

¹⁶ The vendor name is usually the payee's Social Security Number.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

This led to erroneous case numbers being input into the Federal Financial System. Under the revised system, each time a case number is entered into the appropriate field of the Federal Financial System, it is validated against a table containing valid case numbers that is updated nightly. While validating case numbers is an important improvement, we believe that the DEA can further strengthen controls by only exporting those case numbers that legitimately should have expenses charged to them instead of all case numbers. Otherwise, under current procedures, expenses can be charged to a case indefinitely. By further enhancing the controls over confidential source payments, the DEA can prevent a closed case from being used to obligate or expend funds.

Audit Trails for the Correction of Data Entry Errors to the CSS Dollar Database. The DEA uses an overlay file to correct errors in the CSS Dollar database. The overlay file overwrites the CSS Dollar data with the corrected information. However, the correction does not leave an audit trail to identify what transactions were affected or what changes were made. Further, according to the Office of Finance, despite the February 2004 enhancements to the Federal Financial System that improved the overall integrity of the data being transferred, the daily upload was still not working properly and was still requiring overlays to correct the data. Therefore, the DEA should continue to correct the interface between the Federal Financial System and the CSS Dollar database and implement an audit trail to identify what changes were made to the electronic records.

Delays in Processing Financial Payments through the DEA Federal Financial System and CSS Dollar database. Additional concerns about the CSS Dollar data include timeliness and reliability. The processing of confidential source payments through the imprest fund, to the Federal Financial System, and into the CSS Dollar database can take up to 17 days. Without current and accurate information, other DEA offices reviewing the CSS Dollar database cannot accurately determine if payments to a confidential source exceeded the calendar year or lifetime levels.

Review of Payments

During our audit, we reviewed 150 confidential source files and documentation of 4,861 DEA payments to confidential sources totaling \$15,101,198 to determine if:

- the transaction type was specified and appeared correct,
- the Budget Object Code was listed and correct,

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103) had a citation to a specific Report of Investigation (DEA 6) found in the confidential source file,
- reimbursements were supported with receipts and the DEA 103 noted expense descriptions,
- all necessary signatures appeared on the DEA 103, and
- appropriate approvals were noted on the DEA 103.

The results of our review are noted in each of the following six subsections.

Transaction Type. During our audit, we noted 413 of 4,861 payments (8 percent), totaling \$757,180, that either did not specify the type of payment, had more than one type of payment specified, or the remarks describing the payment did not correspond to the payment type selected. Even though these 413 payments either were incomplete (no box checked) or in error (the remarks did not correspond with type of payment selected), a supervisor approved them. Such errors would make it difficult to accurately respond to a prosecutor's request to list payments to a confidential source by type of payment.

Budget Object Codes. During our review of payments at Los Angeles, Phoenix, Houston, and Chicago, we noted 1,632 out of 4,097 (40 percent) payments, totaling \$2,959,724, that were in error or did not have fund citations on the copy of the DEA 103 that was distributed to the establishing office's confidential source file. Therefore, we could not verify that the payments were accurately recorded in the Federal Financial System.

Reference to a Specific Report of Investigation (DEA 6). The DEA Agent Manual states that in completing the DEA 103, the agent must include a brief synopsis of the basis or justification for the payment, the source of funds (if funding was provided by another agency), and a citation to the DEA 6 or teletype that explains or justifies the payment. During our review of files in New York and Miami, we noted that in 11 of 24 confidential source files (45 percent) we reviewed, the DEA 103s either did not specify a DEA 6 or the form could not be located in the confidential source file. In those cases we could not determine the basis or justification for the payment.

During our review of files in Los Angeles, Houston, Phoenix, and Chicago, we expanded our review to identify any DEA 103 that either did not identify a DEA 6 or the form specified was not in the confidential source file.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

We determined that one-third of all payments either did not identify a specific DEA 6 or the form specified could not be located in the confidential source file or in the agent's personal files. In those cases, we could not determine the basis or justification for the payment. Given the wide latitude agents have in determining the amount of payments and the confidential nature of the transactions, the justification for the payment should be specifically identified. Without a specific justification, the DEA 103 is not complete and supervisory officials could not accurately determine if the payment is reasonable or appropriate.

Reimbursement Receipts and Expense Descriptions. During our review of confidential source files in New York, Miami, Los Angeles, Phoenix, Houston, and Chicago, we reviewed 1,332 payments for reimbursements of expenses to determine if they were supported with receipts. We found that receipts were included for only 3 percent of the reimbursement payments. In addition, when reviewing reimbursement payments, we examined the description noted in the remarks field of the DEA 103. We found that 775 of 1,332 reimbursement payments either had no description of the expenditure or generic descriptions such as "expenses incurred" or "U/C expenses." It is important that the expense description be specific given the wide latitude agents have in determining the amounts of the payments and the confidential nature of the transactions. The lack of receipts and the inadequate descriptions of the expenses create a lax internal control environment where payments may be approved that are not reasonable, appropriate, or justified. We believe that the DEA supervisors need to improve their oversight over reimbursements.

Approvals. The DEA Agent Manual requires that a second-line supervisor or above approve payments greater than \$2,500, and a Senior Executive Service-level manager and the designated Headquarters personnel from either the Office of Domestic Operations or the Office of International Operations approve payments greater than \$25,000. According to the Unit Chief of the Confidential Source Unit, a Receipt for Cash or Other Items (DEA 12) should be attached to the DEA 103 if the required supervisor approval of the payment is on the DEA 12. However, the DEA Agent Manual does not require the DEA 12 to be in the confidential source file.

During our audit work in New York and Miami, we noted that the DEA 12 forms generally were not found in the confidential source files. Therefore, in Los Angeles, Houston, Phoenix, and Chicago, we expanded our testing by requesting the DEA 12s if they were not found in the confidential source file. In Los Angeles, Phoenix, Houston, and Chicago, we reviewed 4,097 payments, of which 439 exceeded \$2,500 and consequently required approval beyond the agent's group supervisor. For 66 of the 439 payments

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

(15 percent) totaling \$1,016,921, the DEA 103 did not reflect the appropriate supervisory approval and the division offices could not locate the DEA 12s to demonstrate appropriate supervisory approval. Without the higher-level manager's approval on or attached to the DEA 103, the document is incomplete and it is unclear whether the appropriate supervisor approved the payment.

Signatures. As part of our audit, we reviewed the DEA 103 forms to determine if: 1) all required signatures were documented on the form, 2) the confidential source signature appeared to be consistent among payments, 3) the witness or supervisor signature was a carbon copy, and 4) the DEA used "white out" for corrections rather than initialing the correction. We generally observed that the payments had all the required signatures, the signatures appeared authentic, the witness and supervisor signatures were carbon copies, and corrections, generally were crossed out and initialed.¹⁷

During our testing, we also noted that 47 of 150 confidential source files we reviewed had signature exemplars for the confidential source.¹⁸ We discussed the issue of signature exemplars with DEA officials in Los Angeles and were told that they are no longer required. In fact, none of the four DEA Agent Manuals in effect since 1987 indicate that signature exemplars are required. However, the signature exemplars made it easier for a reviewer to validate the confidential source's signature, and we believe signature exemplars represent an additional internal control and best practice that the DEA should consider requiring.

Conclusion and Recommendations

This audit identified areas where the DEA can improve its risk management over the use of confidential sources. We found that Initial and Continuing Suitability Reports and Recommendations were not adequately documented. These assessments are important in assessing the risks of utilizing a confidential source and should determine the nature and extent of confidential source monitoring. We also found instances where multiple DEA

¹⁷ We observed the use of "white out" on 23 original payment documents. The use of white out obscures the information that is being corrected. The practice of crossing out the error and initialing the correction is the generally accepted method of correcting original documents because it does not obscure the information being corrected.

¹⁸ Signature exemplars are documents that provide samples of an individual's written signature. The signature exemplars would aid in verifying the confidential source's signature on payments. We observed signature exemplars in Phoenix (6 of 30), Washington (16 of 16), and Chicago (25 of 25) confidential source files.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

offices categorized the same source differently and improperly categorized other sources. In addition, we found that the DEA's new category of paid confidential sources - Limited Use confidential source - eliminated critical documentation needed to adequately assess the risk of utilizing these sources. Further, the Sensitive Activity Review Committee's failure to independently review and evaluate underlying suitability data diminishes the value of this high-level oversight function.

We also concluded that the DEA does not have an effective system that accounts for and reconciles all confidential source payments. During the audit, historical confidential source total payment information materially changed each time the DEA's system was queried. Further, the DEA relies on a manual process to provide payment information during discovery and to determine if payments to confidential sources exceeded calendar year and lifetime caps. Specifically, Confidential Source Coordinators must contact multiple offices that have used a confidential source in order to accurately calculate all payments. This manual process is time-consuming, prone to error, and could adversely affect DEA's ability to provide accurate confidential source payment information.

We developed 12 recommendations to help the DEA improve its management of confidential sources. Among these recommendations are for DEA to:

1. Update the DEA Agent Manual to
 - a. Require comprehensive written Initial Suitability Reports that address all of the factors specified in the Attorney General Guidelines.
 - b. Require written continuing suitability reports that address all the factors specified in the Attorney General Guidelines.
 - c. Require that the Sensitive Activity Review Committee either review the confidential source files for all long-term confidential sources, or review the written Initial and Continuing Suitability Reports and Recommendations and document their findings.
 - d. Clarify the process for establishing Limited Use confidential sources to include demonstrating how the DEA can be assured the individual is eligible for Limited Use status and how this status either complies with or is exempt from the Attorney General Guidelines.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

2. Implement a policy of documenting the rationale for a confidential source's categorization.
3. Add a module to the Confidential Source System that tracks confidential source Impeachment Information.
4. Account for all payments made to a confidential source by the DEA, not just payments using DEA-appropriated funds.
5. Enhance controls over confidential source payments to prevent a deactivated confidential source or administratively closed case from being used to obligate or expend funds.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

**THE DRUG ENFORCEMENT ADMINISTRATION'S
PAYMENTS TO CONFIDENTIAL SOURCES**

TABLE OF CONTENTS

	Page
INTRODUCTION	1
FINDINGS AND RECOMMENDATIONS	9
I. THE DEA CAN IMPROVE RISK MANAGEMENT OVER THE USE OF CONFIDENTIAL SOURCES	9
RECOMMENDATIONS	22
II. THE DEA LACKS AN EFFECTIVE AND ACCURATE CONFIDENTIAL SOURCE PAYMENT SYSTEM	23
RECOMMENDATIONS	47
STATEMENT ON THE INTERNAL CONTROLS	49
APPENDIX I - OBJECTIVES, SCOPE, AND METHODOLOGY	50
APPENDIX II - DEA FORMS	52
APPENDIX III - CONFIDENTIAL SOURCE CATEGORIZATIONS	63
APPENDIX IV - SUITABILITY FACTORS	65
APPENDIX V - UNSATISFACTORY COOPERATION OR BEHAVIOR OF A CONFIDENTIAL SOURCE	67
APPENDIX VI - BUDGET OBJECT CODE DEFINITIONS	69
APPENDIX VII - PAYMENTS DOCUMENTED AT FIELD SITES	70
APPENDIX VIII - THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS	74
APPENDIX IX - DEA RESPONSE TO THE DRAFT AUDIT REPORT	107
APPENDIX X - OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT	120

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

INTRODUCTION

The mission of the Drug Enforcement Administration (DEA) is to enforce the controlled substance laws and regulations of the United States and investigate those organizations involved in the growing, manufacture, or distribution of controlled substances. A valuable tool used by the DEA to combat drug crime is confidential sources.¹ DEA officials view confidential sources as the "bread and butter" of the organization and state that without them the DEA could not accomplish its mission. Although confidential source payments represent a small percentage (about 2 percent) of the DEA's total Fiscal Year (FY) 2005 budget of \$2.15 billion, confidential sources are significant to initiating investigations and providing information or services to facilitate arrests and seizures of drugs and cash.² According to the DEA, it has about 4,000 active confidential sources at any one time, and more than 113,000 have been activated since 1996.³

Background on DEA Confidential Sources

Managing confidential sources presents significant challenges, because the DEA must interact with and rely on information from people whose credibility may be questionable, but who also may provide the key to a successful criminal investigation.

Confidential sources come from all walks of life. For example, some sources are concerned law-abiding citizens who are trying to clean up their neighborhoods; while others are also law-abiding citizens, but because of the nature of their work, they find themselves

¹ The Attorney General Guidelines use the term "Confidential Informant," while the DEA now uses the term "Confidential Source." DEA previously used the term "Informant" as noted in the DEA Agent Manual (in effect until September 10, 1998) and the form DEA 356 is called an Informant Payment Record. The terms "Confidential Source" and "Confidential Informant" are essentially the same and refer to any individual who provides useful and credible information to a Department of Justice (DOJ) law enforcement agent regarding criminal activities, and from whom the Justice law enforcement agent expects or intends to obtain additional, useful and credible information regarding such activities in the future. Despite the different terms, we used the term "Confidential Source" throughout this report.

² Our calculation is based on the average payments to confidential sources from Fiscal Years (FY) 1998 - 2002 as provided by the DEA. As discussed in Finding II, however, the DEA does not maintain an effective system for determining payments to confidential sources. Therefore, our calculation may not accurately reflect the total amounts paid to confidential sources.

³ By way of comparison, the DEA had over 5,000 Special Agents authorized in FY 2004.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

closer to criminals than the average person. A confidential source can also be a person who is or has been part of a criminal group. Such a person is in a position to reveal the details of a past crime or plans about future crimes, and may also provide significant information that can help to develop an accurate picture of a criminal act.

Before deciding whether to utilize information provided by a confidential source, the DEA must determine that the benefits outweigh the identified risks. A credible source is one who has a record of providing essential information or participating in past activities that have led to drug seizures or arrests. Consequently, confidential sources are sometimes placed in risky and dangerous situations. For example, a confidential source may purchase or transport drugs, introduce an undercover agent to the target of a criminal investigation, or meet with the target himself. Despite these risks, confidential sources are motivated by many factors, including fear, financial gain, avoidance of punishment, competition, and revenge. These factors must constantly be balanced against the credibility of a confidential source.

The DEA paid confidential sources approximately \$30 - \$35 million per year from FY 1998-2002. As shown in the following table, the payments are categorized as specific types, including Securing of Information (payments for information and reimbursements of expenses), Payments to Foreign Police Officials, Rewards to Informants, Witness Temporary Relocation and two types of Asset Forfeiture Awards.⁴

⁴ Appendix VI lists the definitions for the types of confidential source payments.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

471CE1

DEA Payments to Confidential Sources⁵

Fiscal Year							Total
1998	\$18,237,343	2,388,367	983,921	118,395	4,671,145	8,319,755	\$34,718,926
1999	\$16,970,922	3,915,395	325,650	39,794	3,839,098	5,919,895	\$31,010,754
2000	\$19,271,253	2,494,013	255,189	65,748	4,143,734	6,604,120	\$32,834,057
2001	\$19,142,035	2,507,827	2,416,340	88,698	6,000,596	4,920,638	\$35,076,134
2002	\$19,019,444	2,993,265	1,949,574	52,193	3,415,916	4,652,032	\$32,082,424

Source: DEA Federal Financial System June 2003

During our audit we requested the DEA to provide us with the lifetime payments for 176 confidential sources we noted during our review of 150 confidential source files and 64 closed investigative case files. We found that 27 of the 176 sources exceeded \$200,000 in lifetime payments, while 10 of the 176 received greater than \$1,000,000. The following table summarizes the information:

Lifetime Payments to Confidential Sources⁵

Lifetime Payments	Number	Percentage
Greater than \$2,000,000	1	1%
Between \$1,000,000 and \$1,999,999	9	5%
Between \$500,000 and \$999,999	2	1%
Between \$200,000 and \$499,999	15	9%
Between \$100,000 and \$199,999	26	15%
Under \$100,000	123	70%
Total	176	100%

Source: DEA Confidential Source System (CSS) Dollar database.

Management of the DEA's Confidential Source Program

The management of confidential sources within the Department of Justice is governed by the Attorney General Guidelines Regarding the Use of Confidential Informants (Attorney General Guidelines).⁶

⁵ As discussed in Finding II, the DEA does not maintain an effective system for determining payments to confidential sources. Therefore, the dollar amounts supplied by the DEA may not accurately reflect the total amounts paid to confidential sources.

⁶ The Attorney General Guidelines were issued in January 2001 and revised in May 2002. See Appendix VIII for the Attorney General Guidelines.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The Guidelines prescribe processes to monitor confidential sources. In short, the revised Attorney General Guidelines:

- Set documentation requirements for the establishment and continued use of a confidential source.
- Require that all payments to a confidential source be commensurate with the value of the information provided. All payments must be witnessed by at least two law enforcement representatives, and the source is required to sign or initial and date a written receipt.
- Require senior field manager approval for payments greater than \$2,500 but less than \$25,000; for payments greater than \$25,000, both a senior field manager and a designated senior headquarters official need to approve the payment. Confidential source payments must be monitored on both an annual and aggregate basis, and any payments exceeding the specified levels need headquarter's approval.

The DEA incorporated the Attorney General Guidelines into section 6612 of the DEA Agent Manual, entitled, "Confidential Sources." This section lists the mandatory requirements for the DEA's Confidential Source Program and sets procedures for establishing, monitoring, and paying sources.

The DEA manages its confidential sources through its field offices. A field office that recruits a confidential source is responsible for debriefing the confidential source, completing the paper work, and supervising the day-to-day oversight of the source. The Command Center at DEA Headquarters determines whether a confidential source was previously established and assigns a unique confidential source number to those who were not.⁷ The Confidential Source Unit, also at DEA Headquarters under the Office of Operations Management, is responsible for the oversight of all confidential source-related programs. The Confidential Source Unit wrote the portion of the DEA Agent Manual related to confidential sources, provides training to the

⁷ The DEA Command Center is operated by Office of Operations Management personnel at DEA Headquarters and is manned by nine shift workers responsible for entering the data into the Confidential Source System (CSS). The Command Center is operational 24 hours a day, 7 days a week.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

confidential source coordinators, and is responsible for the maintenance of the Confidential Source System (CSS).⁸

In addition, the DEA's Office of Inspections reviews the Confidential Source Program at each DEA office on a 3-year cycle. A typical inspection includes:

- Interviewing confidential sources about how long they have worked with the DEA, the payment process and how much they have received, if they have been arrested or detained since working with the DEA, and if they have testified in a court proceeding. Confidential sources are chosen at random; however, an attempt is made to interview those sources who received large payments or those sources working on Attorney General Exempted Operations.⁹
- Examining confidential source payments to ensure they are supported by documentation and were approved according to

⁸ In addition to the training that is provided to the field Division's confidential source coordinators, the DEA provides confidential source management training through its Professional Development Program. The Confidential Source Management School, which is coordinated by DEA's Office of Training, is a three-day program that is delivered to DEA field divisions throughout the year to provide DEA Special Agents, Diversion Investigators, and Intelligence Research Specialists with the skills and knowledge necessary for managing confidential sources. The course is designed to address problems with confidential sources. It focuses on confidential source policies and recruitment and management of high-profile and high-risk sources.

The CSS is an automated, limited access database containing a record of all confidential sources assigned a DEA confidential source number. The CSS contains confidential source information input by DEA Headquarters personnel from the Confidential Source Establishment Form (DEA 512), Deactivation reports, and the Quarterly Management Reviews of Confidential Source Utilization. The Quarterly Management Reviews of Confidential Source Utilization are supposed to detail biographical changes, changes in physical appearance, and the current controlling and supervising agents. A separate database module - CSS Dollar - records payments to confidential sources and is populated with information from the Federal Financial System.

⁹ The Department of Justice Appropriation Act of 1980 (Public Law 96-132) initially authorized the DEA and the Federal Bureau of Investigation (FBI) to use appropriated funds to establish certain undercover operations. Attorney General Exemption is required before undercover operations personnel can purchase or lease property, acquire or operate proprietary corporations or businesses, deposit funds in financial institutions, or use the proceeds from operations to offset necessary and reasonable expenses.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

the levels of authority required by the DEA Agent Manual. The inspection, however, makes no judgments on whether payments are commensurate with the value of the information.

- Auditing imprest fund controls concerning the handling and accountability of cash, required documentation, and separation of duties.¹⁰
- Reviewing files to ensure that quarterly management reviews were conducted by first-line supervisors; all required documents are in the confidential source file; information in the files support the source's suitability assessment; and documents identify confidential source activities that support a payment.

We reviewed the DEA Inspection findings relative to imprest fund and the confidential source program for FY 2000-2002. In reviewing the reports, we noted certain issues of concern, but we did not observe a pattern documenting widespread problems. Findings noted in the imprest fund audits included: (1) some Receipts for Cash or other Items (DEA-12s) were not recorded or cleared within timeframes specified; (2) required audits were not performed on the imprest fund; (3) approvals were inappropriate or missing; and (4) imprest funds were used for other than the purchase of evidence or information. Findings in the confidential source program included: (1) categorizing a confidential source as regular use when the source had a criminal record, (2) Vouchers for Purchase of Evidence or Payment to Confidential Source (DEA-103) did not provide justification for payments, (3) Quarterly Management Reviews were either not completed or documented, (4) appropriate second line approval was not obtained when required, and (5) the confidential source files did not contain the initial debriefing or the Confidential Source Agreement (DEA-473) when required.

¹⁰ An imprest fund is a fixed-cash fund that is advanced to DEA cashiers, who in turn advance cash for Purchase of Evidence or Purchase of Information, "flash rolls," and other mission-related expenses. The DEA also can pay confidential sources out of non-appropriated imprest funds such as High Intensity Drug Trafficking Area funds. These non-appropriated imprest funds have a fiduciary outside of DEA, but DEA agents may provide funds to DEA confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

FINDINGS AND RECOMMENDATIONS

I. The DEA Can Improve Risk Management Over the Use of Confidential Sources

Our audit identified areas where the DEA can improve its risk management over the use of confidential sources, including enhancing documentation required by the Attorney General Guidelines. We found that Initial and Continuing Suitability Reports and Recommendations were not adequately documented. These assessments are critically important in assessing the risks of utilizing a confidential source and should determine the nature and extent of confidential source monitoring. We also found instances where multiple DEA offices classified the same source differently and improperly classified other sources. In addition, the DEA added a new category of paid confidential sources - Limited Use Confidential Source - and does not require a background review or other documentation needed to adequately assess the risk of utilizing these sources. In addition, the Sensitivity Activity Review Committee's reliance on the Headquarters Confidential Source Unit and Special Agents in Charge to review and assess long-term confidential sources diminishes the value of the required independent, high-level oversight function.

Although the use of confidential sources can be beneficial in assisting the DEA in investigating criminal activity, confidential sources, by their nature, present management challenges. For example, accountability and transparency of transactions are normal traits of good internal controls and deterrents to fraud, waste, and abuse. However, the clandestine nature of confidential transactions challenges an organization to develop a system of checks and balances that protects the covert nature of the transaction while at the same time providing assurance that the expenditure is reasonable, necessary, and in accordance with applicable policies and regulations.

Press accounts of misconduct by sources and their case agents have placed the system for managing informants into the spotlight. While the most infamous case of informant misconduct, [REDACTED] involved the FBI, the DEA had some highly publicized

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

issues regarding informants.¹⁴ Specifically, the DEA's experience with confidential source [REDACTED] demonstrates the special care needed to carefully evaluate and closely supervise confidential sources. (b)(7)(C)

The secrecy and risks surrounding the use of confidential sources challenge the DEA to ensure that sources are not only credible, but also that agents do not develop close financial or personal relationships with sources that could compromise a case. Managing confidential sources requires the DEA to constantly assess the risk for each source it utilizes. In the context of confidential sources, risk assessment is the continual identification and analysis of relevant adverse factors that are weighed against the potential benefit of using the source. Although the DEA adopted policies and procedures to manage the risk of using confidential sources, we found that the DEA could improve its risk management in the following areas: 1) initial suitability reporting and recommendations, 2) categorization of confidential sources, 3) continuing suitability reporting and recommendations, 4) review of long-term confidential sources, and 5) maintenance of impeachment information.¹⁵

Initial Suitability Reporting and Recommendations

The Attorney General Guidelines outline requirements that the DEA must fulfill before activating a confidential source. Specifically, case agents for confidential sources need to complete and sign a written Initial Suitability Report and Recommendation that addresses specific factors, or indicate on the report that a particular factor is not applicable. The DEA Agent Manual states that suitability statements need not consist of more than one paragraph, but must detail the (b)(7)(D), (C)

14 [REDACTED]

¹⁵ Impeachment information may include payments to the confidential source, any oral or written agreements between the DEA and the confidential source, and any information known by the DEA that may affect the credibility of the confidential source. Examples of impeachment information are a confidential source's criminal record, a substance abuse problem, or instances where the confidential source has given false testimony or statements.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

specific benefits of utilizing the source with the identified risk factors.



During our audit, we tested 150 confidential source files to determine if written initial suitability risk assessments were completed. Of the 150 files reviewed, 63 confidential sources were activated after the January 2001 effective date of the Attorney General Guidelines. Our testing revealed that only 28 of 150 (19 percent) confidential source files contained written initial suitability risk assessments addressing the specific risk assessment factors. Further, only 10 of the 63 confidential source files (16 percent) activated after January 2001 requirement contained written initial suitability assessments addressing the specific risk assessment factors. Of the three Division offices we first visited, we found that written initial suitability risk assessments generally were completed in the Washington, D.C., and New York offices, but not in the Miami office. We subsequently expanded our testing in the Los Angeles, Phoenix, Houston, and Chicago offices (110 of the 150 confidential source files reviewed) to determine if the suitability factors were addressed in other documents besides a formal risk assessment. Our results are summarized in the following table:

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

**Evidence in the 110 Confidential Source Files
Concerning Suitability Factors**

Suitability Factors	Documentation in the File	Documentation not in the File	Percentage Documented
Criminal background checks	105	5	95%
Age	110	0	100%
Allen status	108	2	98%
Public Official	48	62	44%
Extent person would use affiliations with legitimate organizations	8	102	7%
Prior record as a witness	11	99	10%
Record as confidential source with other law enforcement agencies	67	43	61%
Reliability and truthfulness	33	77	20%
Motivation	40	70	36%
Alcohol or substance abuse	17	93	15%
Extent to which the information would be relevant to present or potential cases	66	44	60%
Extent information can be independently corroborated	15	95	14%
Relationship of confidential source to the target of the investigation	27	83	25%
Risk the person might adversely affect an investigation or prosecution	11	99	10%
Pose a danger or threat to public, or is a flight risk	11	99	10%
Relative of law enforcement employee	13	97	12%
Risk of physical harm to the confidential source	12	98	11%

Source: OIG review of confidential source files

We found that biographic information such as age, allen status, and contact information was generally included on the Confidential Source Establishment Forms (DEA 512). For other suitability factors, such as the ones noted in the table, information regarding these attributes was not readily apparent. However, we found some of the information on a variety of documents, including the DEA 512 and the Reports of Investigation Form (DEA 6). As a result, during our audit we needed to review the entire confidential source file in order to address some of the factors. This same time-consuming process must

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

be used by DEA agents and supervisors who were not present during the initial establishment of the confidential source so that they are aware of the answers to the suitability factors.

The majority of DEA 512's we reviewed had general statements indicating, in essence, that the benefits of using the confidential source outweighed the risks, without specifying either the benefits or the risks. Examples of these statements included:



These descriptions do not meet the DEA Agent Manual or the Attorney General Guidelines requirements that suitability statements detail the specific benefits of utilizing the confidential source despite the identified risk factors.

Moreover, DEA training information supplied to the OIG by the DEA Confidential Source Unit stated that written risk assessments of potential confidential sources were not required and were to be performed at the discretion of the Special Agent in Charge. In fact, the Los Angeles office had a formal divisional order that stated agents were not to write risk assessments, and the New York office also had guidance that stated a separate written risk assessment was no longer necessary. The Miami Special Agent in Charge waived the requirement to document risk assessments. The fact that DEA does not require a written suitability report that addresses all the specific factors means the DEA Agent Manual is not in compliance with the Attorney General Guidelines.

Initial suitability statements should explicitly provide the reasons for using a confidential source despite adverse information developed. We believe that a written comprehensive initial suitability risk assessment is critical to measuring the benefits of utilizing a confidential source, and it could help other agents who want to use a confidential source but may be unaware of pertinent derogatory information concerning the source. In addition, such a risk assessment is important because it should determine the nature and extent of confidential source monitoring.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Categorization of Confidential Sources

As discussed in the Introduction, how a confidential source is categorized determines the nature and extent of monitoring required by a case agent.

Despite the importance of appropriately categorizing a confidential source, the DEA does not require agents to document their rationale for how a source is categorized. Our discussion pertaining to confidential source categorization revolves around documenting the rationale for categorizing confidential sources and establishing the Limited Use confidential source.

Categorization Rationale. During our audit, we reviewed 150 confidential source files and, as discussed below, questioned 21 categorization decisions:

¹⁸ See Appendix III for a listing of the DEA categories of confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE



Our concern with the categorization of these sources is primarily over the lack of specific information. Although we realize that many confidential sources have a history of criminal activity, these cases highlight the need for documented, specific information to support the categorization of confidential sources. Categorization is important because it determines the amount of monitoring the DEA performs on the individuals. Restrictions must be designed to reduce potential risk to the DEA and must be documented in the confidential source file. If the DEA does not adequately monitor or restrict a confidential source, that source may jeopardize an investigation.

Limited Use Confidential Source. In the wake of the September 11, 2001, terrorist attacks, the DEA added this new category of confidential sources, which eliminated certain documentation requirements. According to the DEA Agent Manual, Limited Use confidential sources must be free of criminal activity or criminal associations and will not be required to testify. In addition, they are paid and must provide information without the direction of the DEA.¹⁸ According to the DEA Agent Manual, if the confidential source meets this definition, the source will not be fingerprinted, photographed, or have an initial debriefing or a suitability statement.

¹⁷ If an individual's presence in the United States is necessary for law enforcement purposes, and the individual would otherwise be ineligible to receive a visa to the United States, entry pursuant to the Significant Public Benefit Parole Program can be made. Additionally, Section 13003 of the Violent Crime Control and Law Enforcement Act of 1994 created a new non-immigrant classification ("S" visa). This visa is valid for 3 years and allows the confidential source and members of the source's family to reside and work in the United States.

¹⁸ A confidential source who independently provides information to the DEA would be working without the direction of the DEA.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The DEA Section Chief of the Confidential Source Unit stated that the DEA created the Limited Use confidential source category to streamline the establishment process and better receive and provide information. Immediately after the terrorist attacks, the DEA was flooded with information from other agencies and tips from private citizens. Some individuals who were defined as a "professional" business person or a "tipster" (concerned citizens who provide information) were reluctant to go through some of the confidential source establishment process such as fingerprinting and photographing. However, the Attorney General Guidelines' minimum documentation requirements for paid sources are:

- A photograph of the source;
- The agencies' efforts to establish sources' true identity;
- The results of a criminal history check;
- The Initial Suitability Report and Recommendation;
- Any promises or benefits, and the terms of such promises or benefits that are given to the source by any federal prosecuting officer or any state or local prosecuting office; and
- All information that is required to be documented in the confidential sources' files pursuant to these Guidelines.

By not photographing, providing an initial debriefing, or performing a written initial suitability risk assessment of a paid confidential source, the DEA is not in compliance with the Attorney General Guidelines. Further, the DEA Agent Manual specifies that the process for determining if a confidential source is suitable begins with an initial debriefing, fingerprinting, and photograph. These processes must be completed before the confidential source classification can be determined. Therefore, the elimination of initial debriefings, fingerprints, photographs, and the suitability statement for Limited Use confidential sources does not correspond to DEA process. In addition, we are unclear how an agent can determine that an individual meets the criteria of Limited Use confidential source without a suitability risk assessment to determine that the individual is a professional business person or tipster and is free from criminal activity or associations. Therefore, we believe the DEA should clarify the process for establishing Limited Use confidential sources by either demonstrating

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

how it can be assured the individual is eligible for Limited Use status, or is exempt from the Attorney General Guidelines.

Continuing Suitability Reporting and Recommendations

In addition to the Initial Suitability Report and Recommendation, the Attorney General Guidelines require, at least annually, the case agent to review the confidential source's file and complete and sign a written Continuing Suitability Report and Recommendation which must be forwarded to a field manager for written approval. The purpose of the Continuing Suitability Report and Recommendation is to determine whether the risk of using a source has changed since the initial evaluation, and whether a confidential source should continue to be utilized.¹⁹ In completing the Continuing Suitability Report and Recommendation, the case agent must address the same factors outlined in the Initial suitability determination (or indicate that a particular factor is not applicable), and indicate the length of time that the individual has been registered as a confidential source and handled by the same agent.

The DEA does not require an annual review. Instead of the annual review, the DEA requires first-line supervisors and controlling agents to perform Quarterly Management Reviews of Confidential Source Utilization (Quarterly Management Reviews) on each active confidential source. According to the DEA Agent Manual, the quarterly review must document:

- [REDACTED]
- possible revisions to the initial risk assessment,
- [REDACTED]
- [REDACTED]

B(7)(E)

B(7)(E)

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- [REDACTED]
- whether the confidential source should remain active.

(B)(7)(E)

The DEA Headquarters Confidential Source Program Manager is supposed to monitor the field divisions to ensure that all Quarterly Management Reviews are completed. The DEA provided us with a template for the reviews, which suggests the format and language of the report, but it does not specify that the first-line supervisor needs to address each continuing suitability factor.

Our review of 150 confidential source files revealed that none of the Quarterly Management Reviews addressed all continuing suitability factors. Although some of the factors were addressed, such as change of address, indication of criminal background checks, or change in phone number, most reviews contained generic or boilerplate statements such as "no changes in biographic information." Given that the Initial Suitability Report is generally not written and does not provide information on all suitability factors, the lack of specific information on the Quarterly Management Reviews makes it even more difficult to ascertain if agents are aware of the risks of using a source and are taking these risks into consideration when determining the suitability of a confidential source.

In addition, when reviewing the Quarterly Management Reviews we noted that:

- The confidential source files generally did not include copies of the most recent criminal check reports. Rather, the Quarterly Management Reviews only included an indication that a check was run.
- Prior to 2002, the Quarterly Management Reviews contained documentation of the calendar year and lifetime payments. After the second quarter of 2002, the DEA discontinued this process. The Section Chief for the Confidential Source Unit indicated this practice was discontinued because it was duplicative.

Although the DEA's Quarterly Management Reviews exceed the Attorney General Guidelines' annual review requirement, the DEA's approach needs improvement. The Attorney General Guidelines require that the DEA address each suitability factor or indicate that a

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

factor is not applicable. The DEA's approach of only indicating "no change" does not provide assurances that the agent has adequately considered whether the benefits of using a source continue to outweigh the risks.

Review of Long-Term Confidential Sources

One of the purposes of the Attorney General Guidelines is to provide more oversight of agents handling confidential sources by having individuals who are not as close to those sources make critical decisions about payments and other matters. The Attorney General Guidelines require a "Confidential Informant Review Committee" to review a confidential source who has been active for more than six consecutive years, to the extent that the source remains active every six years thereafter. The Guidelines also state that the Confidential Informant Review Committee must review the confidential source's completed Initial and Continuing Suitability Reports and Recommendations, and decide whether, and under what conditions, an individual should continue to be used as a confidential source.

To comply with the Attorney General Guidelines, the DEA created its own Sensitive Activity Review Committee.²⁰ This Committee convenes not only to review long-term confidential sources, but also to discuss issues regarding property, money laundering, and proprietary storefront operations.

The Undercover and Sensitive Operations Unit Chief stated to the OIG that prior to November 2003, the Committee had not reviewed any matters pertaining to DEA long-term confidential sources. He also stated that the Committee does not review confidential source files. Instead, it reviews an Excel spreadsheet prepared by the Confidential Source Unit that contains names and other pertinent information about long-term confidential sources. He further stated that the Confidential

²⁰ The Undercover and Sensitive Operations Unit is part of the Office of Enforcement Operations. According to the Undercover and Sensitive Operations Unit Chief, who is a permanent member of the Sensitive Activity Review Committee, a variety of individuals contribute to the Sensitive Activity Review Committee, including the Chief for Domestic Operations, the head of the Narcotics and Drug Operations, Office of Internal Affairs, representatives from the Department of Justice, the Domestic Chief Counsel, the Asset Forfeiture and Money Laundering Coordinator, and the International Chief Counsel for Foreign Operations. According to the Attorney General Guidelines, the representatives from the Department of Justice are appointed by the Assistant Attorney General for the Criminal Division. They are a Deputy Assistant Attorney General for the Criminal division and an Assistant United States Attorney.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Source Unit Section Chief is available to answer questions that arise that cannot be explained by the information contained in the spreadsheet. Although a Committee member may review a confidential source file upon request, the Unit Chief stated that he does not believe this is necessary. He also stated that the Committee is unlikely to question the judgment of a Special Agent in Charge who has already reviewed the information in the confidential source file.

In our judgment, the DEA should strengthen its management over long-term confidential sources. The Sensitive Activity Review Committee should conduct a high-level, independent review of long-term confidential sources. The review should monitor not only the controlling agents' decisions, but also the actions of supervisors in the chain of command, including the Special Agent in Charge and any DEA Headquarters staff. If the Committee relies solely on Special Agents in Charge and the Headquarters Confidential Source Unit without independently reviewing the information itself, we believe the value of its work is significantly diminished.

DEA Maintenance of Impeachment Information

The DEA Agent Manual requires agents to provide prosecutors with all discoverable information pertaining to any confidential source who may be utilized as a witness. This information includes payments to the confidential source, any oral or written agreements between the DEA and the confidential source, and any impeachment information known by the DEA that may affect the credibility of the confidential source. Examples of impeachment information are a confidential source's criminal record, a substance abuse problem, or instances where the source has given false testimony or statements.

As noted earlier in this report, the DEA does not detail by factor the confidential source's suitability either when initially establishing the source or during the quarterly review. Therefore, it may be difficult for an agent who was not present at either the establishment or quarterly briefing of a source to discover impeachment information about the source.

During our audit, one DEA Confidential Source Coordinator suggested that the DEA develop a central repository of all impeachment information. Such a database would provide anyone who utilizes the confidential source to be aware of all impeachment information about the source without having to manually search multiple files. This could eliminate the current process of manual file

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

checks and it would be a valuable resource to agents who are trying to establish a confidential source in a new office or reactivate one who was previously deactivated. In addition, by implementing a central repository of impeachment information, DEA agents will be better able to determine whether a confidential source should be utilized.

Recommendations

We recommend that the DEA:

1. Update the DEA Agent Manual to
 - a. Require comprehensive written Initial Suitability Reports that address all of the factors specified in the Attorney General Guidelines.
 - b. Require written continuing suitability reports that address all the factors specified in the Attorney General Guidelines.
 - c. Require the Sensitive Activity Review Committee to either review the confidential source files for all long-term confidential sources, or review the continuing written Initial and Suitability Reports and Recommendations, and document their findings.
 - d. Clarify the process for establishing Limited Use confidential sources to include demonstrating how the DEA can be assured the individual is eligible for Limited Use status and how this status either complies with or is exempt from the Attorney General Guidelines.
2. Implement a policy of documenting the rationale for confidential source's categorization.
3. Consider adding a module to the Confidential Source System that tracks confidential source Impeachment Information.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

II. The DEA Lacks an Effective and Accurate Confidential Source Payment System

The DEA does not have an effective and accurate system that accounts for and reconciles all confidential source payments. During our audit, historical confidential source total payment information materially changed by as much as \$14 million each time the DEA's system was queried. Because of the inaccuracy of the automated system, the DEA relies on a manual process to provide payment information during discovery and to determine if payments to confidential sources exceed calendar year and lifetime caps. Consequently, Confidential Source Coordinators must contact multiple offices that have used a confidential source in order to accurately calculate all payments. This manual process is time-consuming, prone to error, and could adversely affect DEA's ability to provide accurate confidential source payment information.

The DEA is required by the Attorney General Guidelines to establish accounting and reconciliation procedures that reflect *all* monies paid to confidential sources. The primary systems utilized by DEA to process and account for confidential source payments are the Federal Financial System and the CSS Dollar database.²¹ Our audit identified deficiencies in the DEA's accounting and reconciliation of confidential source payments that led us to conclude that the DEA does not have an effective and accurate payment system. Specifically, we found inconsistencies in the amounts and types of payments made to confidential sources; deficiencies with the accounting and monitoring of calendar year and lifetime payments; problems with the systems used to account for confidential source payments; and control breakdowns that indicate closer supervisory oversight of confidential source payments is needed.

²¹ The Federal Financial System is a Department of Agriculture system that handles the DEA financial information on a contract basis. The DEA utilizes the Federal Financial System to process confidential source payments. The CSS Dollar database is a subsystem of the DEA's Confidential Source System. The purpose of the CSS Dollar database is to account for monies paid to confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Discrepancies in the Amounts and Types of Payments to Confidential Sources

As part of our review to assess how the DEA accumulates confidential source payment information, we asked the DEA's Office of Finance to provide us with the total amount of Confidential Source payments from FY 1998 through FY 2002 by budget category. The DEA's Office of Finance queried the Federal Financial System in July 2002 and June 2003 and provided us with different payment amounts regarding the same time period. Our review of the payments revealed significant discrepancies in the amounts and types of payments provided to confidential sources as shown in the following table.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

B(7)(E)

**Comparison of Historical
Confidential Source Payment Information**

FY 1998:						
July 2002	\$17,932,802	\$0	\$976,322	\$97,719	\$4,676,145	\$8,291,265
June 2003	\$18,237,343	\$2,388,367	\$983,921	\$118,395	\$4,671,145	\$8,319,755
Discrepancy	\$304,541	\$2,388,367	\$7,599	\$20,676	\$5,000	\$28,490
FY 1999:						
July 2002	\$16,885,001	\$0	\$325,647	\$39,839	\$3,901,098	\$5,891,315
June 2003	\$16,970,922	\$3,915,395	\$325,650	\$39,794	\$3,839,098	\$5,919,895
Discrepancy	\$85,921	\$3,915,395	\$3	\$45	\$62,000	\$28,580
FY 2000:						
July 2002	\$19,110,333	\$0	\$250,408	\$65,248	\$4,134,434	\$6,514,120
June 2003	\$19,271,253	\$2,494,013	\$255,189	\$65,748	\$4,143,734	\$6,604,120
Discrepancy	\$160,920	\$2,494,013	\$4,781	\$500	\$9,300	\$90,000
FY 2001:²⁴						
July 2002	\$19,006,761	\$0	\$2,409,769	\$88,697	\$5,986,800	\$4,828,738
June 2003	\$19,142,035	\$2,507,827	\$2,416,340	\$88,698	\$6,000,596	\$4,920,638
Discrepancy	\$135,274	\$2,507,827	\$6,571	\$1	\$13,796	\$91,900

Source: DEA Federal Financial System. The payment information was supplied in July 2002 and June 2003. The amounts do not include payments DEA made using non-appropriated funds such as High Intensity Drug Trafficking Areas (HIDTA).

When we asked the DEA to confirm the June 2003 summary of confidential source payments as final figures, we were informed that:

²² See Appendix VI for a description of the Budget Object Codes used to pay confidential sources.

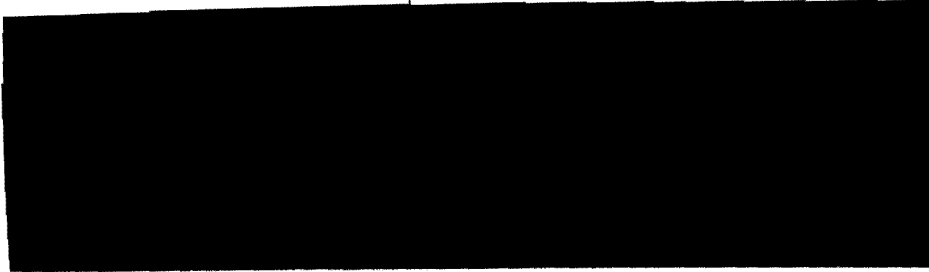
²⁴ In April 2003, the DEA Office of Finance provided detailed transactions regarding FY 2001 confidential source payments. The total of the detailed transactions for FY 2001 was \$11 million less than the total amount supplied in July 2002 and \$14 million less than the total amount supplied in June 2003.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The query run for the OIG by the Office of Finance was run out of the Federal Financial System, as was the query provided at the entrance conference. Because errors in the Federal Financial System may be made at any time and reconciliations completed quarterly, the DEA can confirm that numbers are correct only as of the day they are run. The DEA cannot certify that these same numbers would result from a query conducted on the day the [OIG] report is issued. The DEA is willing to re-run the query closer to the report publication date, but can only confirm those numbers as of the date the query is run.

We are concerned by the degree of inconsistencies in the payment information because historical data should not change significantly over time. Changes to historical data years after the close of a fiscal year call into question the reliability of the data and the system.



B(7)(F)

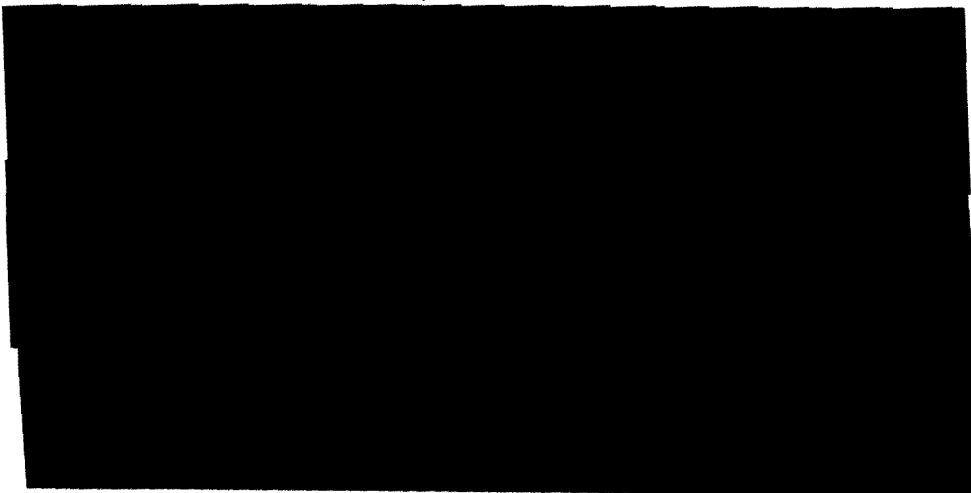


B(7)(F)

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- The Office of Finance does not require a Geographic Drug Enforcement Program and case number to be entered into the Federal Financial System.²⁵ These fields are required for confidential source payments.
- The payment is coded OM, which indicates all other transactions, rather than OP, which indicates Purchase of Evidence/Purchase for Information. The difference in coding specifies that the payments are reimbursed out of a different imprest fund than the one used for Purchase for Information.



(b)(7)(E)

The discrepancies in payments to [REDACTED] were not the only inconsistencies we identified. We also identified problems in the following areas that impact the DEA's ability to provide accurate confidential source payment information: accounting for confidential source payments using non-appropriated HIDTA funds, monitoring calendar year and lifetime payments, problems with the Federal Financial System and the CSS Dollar database, and control issues related to confidential source payments. These problem areas contributed to the inaccurate payment information DEA supplied during the audit and will impact the DEA's ability to monitor both the calendar year and lifetime confidential source payments as required by the Attorney General Guidelines.

(b)(7)(E)

²⁵ The Geographic Drug Enforcement Program is a DEA code that indicates type of investigation, drug, and target.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Accounting and Monitoring of Annual and Aggregate Payments²⁶

The DEA is limited by the Attorney General Guidelines on the amount of money it can pay to a confidential source without receiving certain approvals:

- *Single Payment Approval.* A single payment of between \$2,500 and \$25,000 per case to a confidential source must be authorized, at a minimum, by a senior field manager. A single payment in excess of \$25,000 per case shall be made only with the authorization of a senior field manager and the approval of a designated senior headquarters official.
- *Annual Payment Approvals.* Payments that exceed an aggregate of \$100,000 within a 1-year period shall be made only with the authorization of a senior field manager and the approval of a designated senior headquarters official. The headquarters official may authorize additional aggregate annual payments in increments of up to \$50,000.
- *Aggregate Payment Approvals.* Payments that exceed an aggregate of \$200,000 shall be made only with the authorization of a senior field manager and the approval of a designated senior headquarters official. After the headquarters official has approved payments to a confidential source that exceed an aggregate of \$200,000, the headquarters official may authorize additional aggregate payments in increments of up to \$100,000.

During our audit of 150 confidential source files and 64 case files, we noted a total of 176 different confidential source numbers. We requested the DEA to provide us with the lifetime payments for these 176 confidential sources. The following table summarizes the information:²⁷

²⁶ The Attorney General Guidelines use the terms "annual payment approvals" and "aggregate payment approvals" when discussing approval levels for payments to confidential sources over a period of time. The *DEA Agent Manual* defines the annual payment approval as "calendar year cap" and the aggregate payment approval as "lifetime caps." These terms are used interchangeably in this report.

²⁷ Without reviewing the confidential source files in every office that utilized these confidential sources, we could not determine if the appropriate approvals were obtained.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Lifetime Payments to the 176 Confidential Sources

Lifetime Payments	Number	Percentage
Greater than \$2,000,000	1	1%
Between \$1,000,000 and \$1,999,999	9	5%
Between \$500,000 and \$999,999	2	1%
Between \$200,000 and \$499,999	15	9%
Between \$100,000 and \$199,999	26	15%
Under \$100,000	123	70%
Total	176	100%

Source: DEA CSS Dollar database. The DEA considers the CSS Dollar system to be unreliable. The CSS Dollar database does not contain confidential source payments using DEA non-appropriated funds.

In our review of 176 confidential sources, 27 of 176 (15.3 percent) had received lifetime payments totaling more than \$200,000. Further, 10 of the 176 (5.6 percent) confidential sources had payments totaling greater than \$1 million.²⁸

In addition, we noted that DEA Headquarters automatically authorized an increase in the calendar year and lifetime payment amounts when an asset forfeiture payment was made. Additionally, we noted no instances in which an office requested an increase in the calendar year or lifetime payment level and that request was denied. Although we are not suggesting that these requests for increases should have been denied, our audit revealed weaknesses with how the DEA accounts for non-appropriated HIDTA funds and monitors calendar year and lifetime payments.

Accounting for Non-appropriated HIDTA Funds. While the DEA Agent Manual generally mirrors the language in the Attorney General Guidelines, it differs in a significant aspect. The Guidelines do not distinguish between appropriated and non-appropriated funds; however, the DEA Agent Manual states that only DEA-appropriated funds will be included in the listings of calendar year and lifetime payments, not all monies paid to a confidential source. The DEA Agent Manual goes on to say that all payments to confidential sources using appropriated funds or funds from other agencies must be documented

B(7)(E)

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

on the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103). But payments using non-appropriated funds - such as HIDTA - are not processed through the Federal Financial System and consequently are not included in the CSS Dollar database of payments. This means that payments using non-appropriated funds are not considered in determining whether payments to a confidential source exceed calendar year or lifetime payment levels. Further, since the confidential source payments using HIDTA funds are not processed through the Federal Financial System, the DEA could not provide us the total confidential source payments using HIDTA funds without extensive manual efforts.

Although HIDTA payments are not processed through the Federal Financial System, the DEA Agent Manual requires documentation of these payments to be provided to the Confidential Source Coordinator for inclusion in the confidential source file. This information would be important in reconciling payments listed in the confidential source file to those listed in the CSS Dollar database and also would impact the calculation of the DEA calendar year and lifetime payments. We inquired as to how the Confidential Source Coordinator knows if a payment is from an appropriated fund source (the DEA imprest fund) or from a non-appropriated fund source (HIDTA imprest fund). DEA personnel provided us with varying explanations ranging from all payments without a fund citation were made with non-appropriated funds to the information is listed on the Informant Payment Record (DEA 356).

Monitoring Calendar Year and Lifetime Caps. In addition to not counting non-appropriated funds towards the calendar year and lifetime caps, we noted other problems with how the DEA monitors annual (calendar) and aggregate (lifetime) caps. During our review, DEA officials said the CSS Dollar database monitors the annual and lifetime caps, and "flags" payments that put a source's totals over the limits. The flag is supposed to signal that headquarters approval is required to exceed the cap; however, it does not prevent the payment.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The DEA instructs agents not to use the CSS Dollar Database when providing payment information to prosecutors. Instead they are supposed to manually search through confidential source file to determine the total amount of payments. The manual search can be time consuming if a confidential source was active in multiple offices. If a source was active in multiple offices, all offices must be identified and, since each office maintains a confidential source file and payment records, that office must review its files manually to calculate a total amount of payments.

We were informed by both the former and current Section Chief of the Confidential Source Unit, numerous DEA agents, and five of the seven Confidential Source Coordinators for the offices we reviewed that the CSS Dollar database is unreliable. Consequently, the Washington, Houston, and Miami divisions maintained their own database to track payments to confidential sources. Although Miami did not indicate that the CSS Dollar database was unreliable, the office nevertheless developed its own internal database to track payments.

The Section Chief for the Confidential Source Unit provided a series of e-mails that outlined the long-standing problems the DEA experienced in populating the CSS Dollar database. These issues contributed to the problems with confidential source Andrew Chambers, where the DEA gave conflicting accounts of amounts paid to Chambers. Further, the e-mails indicated time lags in processing the payments, a lack of quality controls, and a communication disconnect between the DEA Office of Finance and the Confidential Source Unit regarding who is responsible for the CSS Dollar database and the importance of correcting the problems. The Section Chief for the Confidential Source Unit said that incomplete records in the data supplied to the CSS Dollar database (incorrect date, case number, and office identifier) make it impossible to perform a proper audit of a confidential source's payment history. We discuss in more detail later the problems with the Federal Financial System and the CSS Dollar database.

To determine if the DEA is monitoring calendar year and lifetime caps, apart from using the CSS Dollar database, we reviewed documentation in the confidential source files for evidence of cap monitoring. Confidential source payments are documented on the Informant Payment Record (DEA Form 356) regardless if the funds are from appropriated or non-appropriated sources. However, this record only lists payments from a specific office and is not a consolidated listing of all payments made by other DEA offices utilizing the same

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

confidential source. Prior to 2002, agents were required to list the calendar year and lifetime payments remaining on the Quarterly Management Reviews, and we observed that this was generally performed. However, in the current version of the DEA Agent Manual (April 2002), the DEA no longer requires that such information be documented in the Quarterly Management Reviews. Instead, the DEA Agent Manual states that the Confidential Source Coordinator and first-line supervisor are to review the payments to determine if they approach the caps.

During our review of 150 confidential source files, we noted that caps were sporadically documented on Quarterly Management Reviews, Receipts for Cash or Other Items (DEA 12), and Confidential Source Establishment (DEA 512). Although we noted a few memoranda requesting cap increases, we did not observe any formal process or consistent practice used by the DEA to monitor calendar year and lifetime caps. We also did not see any formal reconciliation of the CSS Dollar database, the Federal Financial System, or the confidential source payment records. The only evidence we observed of any reconciliation attempts were a few printouts of CSS Dollar payment information and DEA letters to prosecutors listing specific confidential source payment information.

The Confidential Source Program Manager indicated DEA Headquarters does not reconcile the payments listed on the Informant Payment Record (DEA 356) to the CSS Dollar database. While he suggested that perhaps field personnel performed this task, he was not aware of a requirement to do so. We also found no evidence of such a requirement.²⁹

Because the CSS Dollar database is unreliable and the DEA does not have a formal or consistent practice to monitor calendar or lifetime

²⁹ The *DEA Agent Manual* specifies that the Confidential Source Coordinator and first-line supervisor must review the confidential source's payment history to determine if the payments were justified and to determine if they approached calendar and lifetime caps. However, we found no requirement in the *DEA Agent Manual* to reconcile the payments in the confidential source file to those in the Federal Financial System, the CSS Dollar database, or to case expenses. The procedures used by the DEA Inspections Unit to periodically review the Confidential Source Program do not include a reconciliation of payments. While the Confidential Source Coordinator position description indicates that the Coordinator should conduct periodic audits to determine if confidential source information is correct and accurately recorded, the Coordinator's performance work plan does not indicate that reconciling the confidential source payments in the file to the CSS Dollar database is a requirement of the position.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

payments, we were unable to determine if confidential source payment caps were exceeded without the appropriate approvals or verify that the DEA was effectively monitoring caps. In addition, because the CSS Dollar database is unreliable and the DEA does not reconcile confidential source payment information, Confidential Source Coordinators must rely on manual calculations to verify that caps are not exceeded and to provide payment information during discovery. This manual process is time-consuming and prone to error since it requires the Confidential Source Coordinators to contact all offices using confidential sources in order to accurately calculate all payments.

Problems with the Federal Financial System and the CSS Dollar Database

In addition to the unreliability of the CSS Dollar database, we also noted problems with the Federal Financial System's vendor and case tables; the lack of audit trails for the correction of data entry errors in the CSS Dollar database; and delays in processing confidential source payments.

Issues with the Federal Financial System Vendor Name, Case Tables, and the Correction of Errors. In order to enter confidential source payments into the Federal Financial System, the DEA requires a "vendor name." Normally, payments to individuals use that person's Social Security Number (SSN) as the vendor name. For example, a reimbursement of expenses to an agent would use the agent's SSN as the vendor name. In order to protect the identity of the confidential source, however, the DEA cannot use the confidential source's SSN. Instead, for confidential source payments, the DEA uses a derivative of the "confidential source number" as the vendor name. Before February 2004, the Federal Financial System did not have an adequate validation process for the vendor name field. For example, if the confidential source payment was coded using the agent's SSN instead of the confidential source vendor name, and included one of the confidential source payment Budget Object Codes [REDACTED] (b)(2) [REDACTED], the payment would be processed. However, this payment would not be identified as a payment to a particular confidential source within the Federal Financial System or in the CSS Dollar database.

The DEA Office of Finance queried the Federal Financial System for fiscal year 2002 and found 79 records where the Budget Object Code was [REDACTED] but the vendor name was

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

not a confidential source vendor name. Additionally, DEA's Office of Finance personnel indicated that inputting a wrong Budget Object Code (i.e., a Budget Object Code that is not a confidential source payment Budget Object Code) in connection with a confidential source was probably a more common error than inputting an incorrect vendor name. These errors prevent the transactions from being extracted into the CSS Dollar database and therefore do not account for some payments to confidential sources. In other words, this error may understate the amount of payments paid to a confidential source both in a specific year and over the lifetime of the source.

In February 2004, the DEA made enhancements to the Federal Financial System that helps correct the problem of invalid vendor type. The Budget Object Codes used for confidential source payments have a vendor type of "I." If the DEA enters data into the Federal Financial System using a Budget Object Code that has a vendor type "I," then only a derivative of the confidential source number can be entered as a vendor name. If the individual entering the data uses a SSN instead, the system instructs the individual to re-enter a valid Budget Object Code-vendor name combination.

While this enhancement better validates vendor names, a problem still exists with the validation system. Once a confidential source is established and a confidential source number is assigned, that source has a vendor name established. However, if that confidential source is deactivated, the vendor name is not deactivated; therefore, a payment could be processed with a deactivated confidential source vendor name.

When we discussed this issue with the DEA, we were told that the Confidential Source Coordinator would catch this problem when the copy of the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103) was filed in the confidential source file. However, even if the Confidential Source Coordinator noted this error when the paperwork was filed, the funds would have already been paid. Consequently we believe the DEA should further enhance the controls over confidential source payments to prevent a deactivated confidential source from being used to obligate or expend funds. This can be done by removing deactivated confidential source vendor names from the validation table.

Another improvement made by the DEA in February 2004 was the validation of the case number field in the Federal Financial System. Previously, only the first five digits of the case number were validated

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

and the remaining four digits could be any combination of numbers up to 9999. This led to erroneous case numbers being entered into the Federal Financial System. Under the revised system, each time a case number is entered into the appropriate field of the Federal Financial System, it is validated against a table containing valid case numbers that is updated nightly.

While validating case numbers is an important improvement, the DEA can further strengthen controls by only exporting those case numbers that legitimately should have expenses charged to them instead of exporting all case numbers. Under current procedures, expenses can be charged to a case indefinitely. For example, the DEA can continue to charge expenses to cases that have been "administratively closed."³⁰ For instance, a DEA Administrative Officer stated that an agent who embezzled funds from the Imprest fund had cited closed cases on his requests for funds. To prevent a closed case from being used to obligate or expend funds in the future, we believe the DEA should further enhance the controls over confidential source payments.

Audit Trails for the Correction of Data Entry Errors to the CSS Dollar Database. In August 2002, the DEA acknowledged and planned to correct 1,500 payments in the Federal Financial System that were not captured in the CSS Dollar database because of data entry errors by field personnel. The DEA explained that corrections to the CSS Dollar database were made via an overlay file, which overwrites the CSS Dollar data with the corrected information. However, the correction does not leave an audit trail to identify what transactions were affected or what changes were made.³¹

In April 2003, the Section Chief of the Confidential Source Unit and the Confidential Source Program Manager (Operation Management) indicated that input errors in the CSS Dollar database were still a problem. Further, according to the Office of Finance, despite the February 2004 enhancements to the Federal Financial System that improved the overall integrity of the data being

³⁰ Administratively closed cases are those in which further investigation is not warranted or the investigation is to be continued in one or more other cases.

³¹ An "audit trail" is the sequence of paperwork that validates or invalidates accounting entries. The term is also used for an electronic or paper log used to track computer activity. When an information system is developed, an audit trail should be built in to ensure that controls are in place and to integrate fraud prevention and detection methods.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

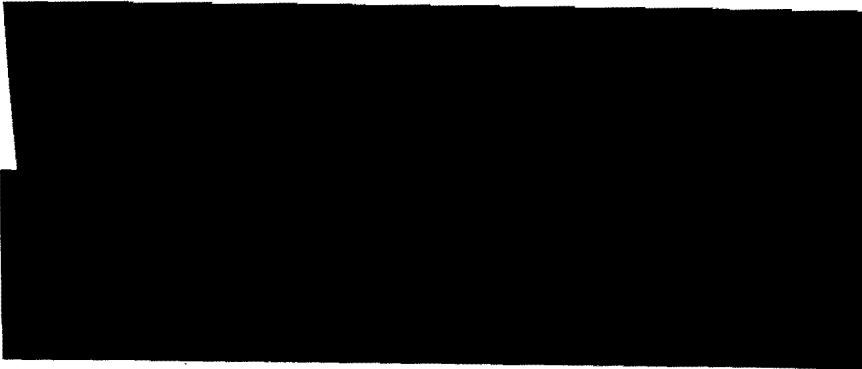
transferred, the daily upload was not working properly and was still requiring overlays to correct the data.

We believe that the DEA should continue to correct the interface between the Federal Financial System and the CSS Dollar database and implement an audit trail to identify what changes were made to the electronic records.

Delays in Processing Financial Payments. Timeliness and reliability of information are other concerns we have about CSS Dollar data. The processing of confidential source payments through the Imprest fund to the Federal Financial System and into the CSS Dollar database can take up to 17 days. The lack of current and accurate information creates the potential for other DEA offices reviewing the CSS Dollar database to be unable to accurately determine if payments to a confidential source exceeded the calendar year or lifetime levels. As a result, payments could be made to confidential sources without receiving the necessary prior approval.

Review of Payments

As part of our review of internal controls over confidential source payments, we reviewed 150 confidential source files and documentation of 4,861 DEA payments to confidential sources totaling \$15,101,198.³² The following chart depicts the number and amount of payments we reviewed from each DEA Division.



B(7)(E)

³² Appendix VII contains the individual confidential source payment summaries of the audit sites. The results include total payments for each office and details the type of payment reviewed.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

The DEA denotes that payments to confidential sources are accounted for in the following Budget Object Codes:³³

[REDACTED] b7(E)
[REDACTED] b(2)
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

During our audit we categorized the 4,861 payments into the categories of payment types noted on the DEA 103, Voucher for Purchase of Evidence or Payment to Confidential Source. In summarizing the 4,861 payments by type of confidential source payment, we observed the most frequent type was for Information/services. The payment type with the most dollars associated with it was an Asset Forfeiture Award - Liquidated Asset (28 USC 524 (C)(1)(C)).³⁴ Further, the award and reward payments were, on average, higher dollar payments but represented a fewer number of payments. The reimbursements payments were, on average, lower dollar payments, but represented a greater number of payments. The following chart depicts the type, number, and amount of payments we reviewed.

³³ See Appendix VI for the descriptions of the Budget Object Codes.

³⁴ See Appendix VI at Budget object code 2579 for a description of Asset Forfeiture- Liquidated Asset.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

(b)(7)(E)

We reviewed payments to determine if:

- the transaction type was specified and appeared correct,
- the Budget Object Code was listed and correct,
- the Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103) had a citation to a specific Report of Investigation (DEA 6) found in the confidential source file,
- reimbursements were supported with receipts and the DEA 103 noted expense descriptions,
- all necessary signatures appeared on the DEA 103, and
- appropriate approvals were noted on the DEA 103.

The results of our review are noted in each of the following six subsections. Some payments were found to be deficient in more than one category, and these deficiencies underscore the DEA's need to improve procedures for the accounting and reconciling of confidential source payments.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

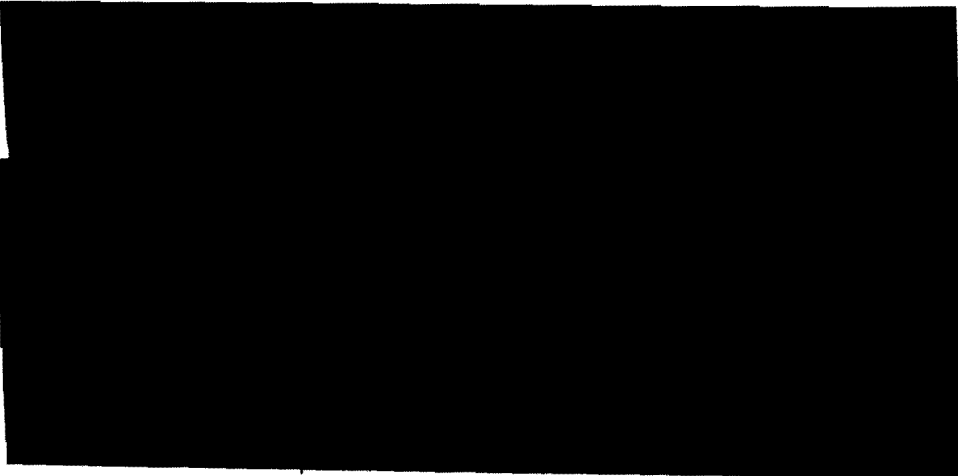
Transaction Type. The Attorney General Guidelines require payment records to specify whether the payment is for information, services, or expenses. The DEA Agent Manual states that an agent may not combine payment types but instead must specify a single type of payment. If an agent pays a confidential source for both information and expenses, two separate Vouchers for Purchase of Evidence or Payment to Confidential Source (DEA 103) need to be completed. During our audit, we noted 413 of 4,861 (8 percent) payments, totalling \$757,180, that either did not specify the type of payment, had more than one type of payment specified, or the remarks describing the payment did not correspond to the payment type selected. Even though these 413 payments either were incomplete (no box checked) or in error (the remarks did not correspond with type of payment selected), a supervisor approved them. Such errors would make it difficult to accurately respond to a prosecutor's request to list payments to a confidential source by type of payment.

Budget Object Codes. According to the DEA Agent Manual, a supervisor must inspect the undistributed DEA 103 to ensure that all copies are properly executed.³⁹ The supervisor's signature on the DEA 103 certifies that the document is properly executed. Additionally, the DEA Financial Handbook states that the fund citation must be listed in section V of the DEA 103.⁴⁰ The current version of the DEA 103 lists various types of payments, such as information services, reimbursement expenses, reward, security, relocation, trafficker-directed funds, and awards. During our review of payments at Los Angeles, Phoenix, Houston, and Chicago, we noted 1,632 out of 4,097 (40 percent) payments, totalling \$2,959,724 that were in error or did not have fund citations on the copy of the DEA 103 that was distributed to the establishing offices confidential source file. Therefore, we could not verify that the payments were accurately recorded in the Federal Financial System.

During our audit, we asked why the fund citation was not on the DEA 103 in the confidential source file. The DEA's Deputy Assistant

³⁹ The DEA 103 is a multi-carbon form. Once the DEA 103 is completed, copies go to the Imprest Fund, Fiscal (accounting), sub-imprest fund (if applicable), division or country office confidential source file, and the establishing office's confidential source file.

⁴⁰ The DEA fund citation is an accounting code that identifies the fiscal year, the fund type, the office requesting the payment, the DEA program code, the office making the payment, and the type of payment (Budget Object Code).



B(7) (E)

Reference to a Specific Report of Investigation (DEA 6).

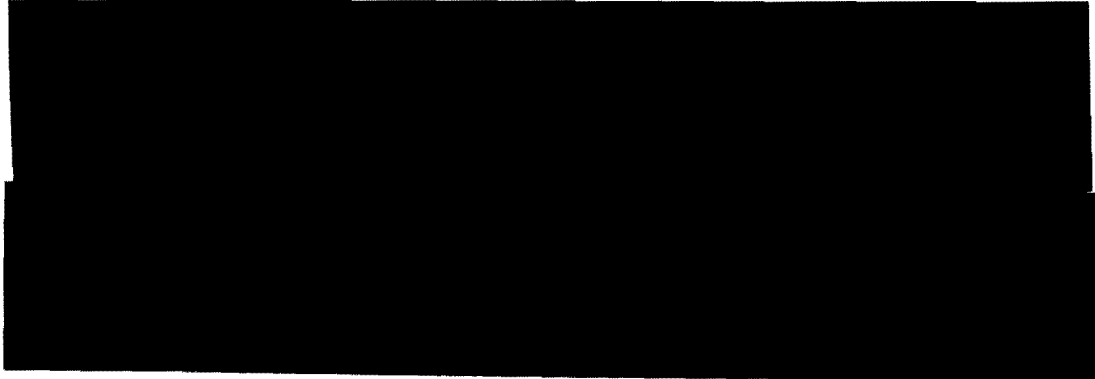
Payment amounts are determined in part by source effectiveness. However, according to the DEA Policy & Planning Section Chief, the DEA has no rating system or objective measurement to assess the success of confidential sources. Agents rely on the number and importance of arrests and leads stemming from the confidential source's information to assess the source's effectiveness. The only guidance the DEA Agent Manual offers in regard to the payment amount is that payments are to be commensurate with information provided.

The DEA Agent Manual states that in completing the DEA 103, the agent must include a brief synopsis of the basis or justification for the payment, the source of funds (if funding was provided by another agency), and a citation to the DEA 6 or teletype that explains or justifies the payment. During our review of files in New York and Miami, we noted that in 11 of 24 confidential source files (45 percent) we reviewed, the DEA 103s either did not specify a DEA 6 or the form could not be located in the confidential source file. In those cases we could not determine the basis or justification for the payment.

During our on-site work in Los Angeles, Houston, Phoenix, and Chicago, we expanded our file review to identify any DEA 103 that either did not identify a DEA 6 or the form specified was not in the confidential source file. As shown in the following table, we determined that one-third of all payments either did not identify a specific DEA 6 or the form specified could not be located in the confidential source file or in the handling agent's personal files. In

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

those cases we could not determine the basis or justification for the payment.



B(7)(E)

Given the wide latitude agents have in determining the amount of payments and the confidential nature of the transactions, the justification for the payment should be specifically identified. Without a specific justification, the DEA 103 is not complete and any supervisory official could not accurately determine if the payment is reasonable or appropriate.

Reimbursement Receipts and Expense Descriptions. The documentation required by the DEA to support reimbursement expenses, such as car rental, hotel, and telephone costs, varied depending on the version of the DEA Agent Manual in effect.

- The DEA Agent Manual in effect from 1987 until September 10, 1998, did not separate reimbursements from payments for information and therefore does not indicate any specific documentation requirements.
- The DEA Agent Manual in effect from September 10, 1998, through June 27, 2001, specified reimbursements as a specific type of payment and stated that reimbursement of expenses incurred by a confidential source should be based upon *actual receipted expenses*.
- The next two versions of the DEA Agent Manual, dated June 28, 2001, and April 24, 2002 (current version), indicated that reimbursements should be based upon actual expenses incurred and required receipts to be obtained

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

whenever possible. The agents were directed to attach the receipts to the establishing office's copy of the DEA 103 in the confidential source file.

The Unit Chief of the Confidential Source Unit stated that agents are instructed to collect receipts if possible, but if a confidential source cannot supply a receipt, agents should note on the DEA 103 why receipts were not available.

During our review of confidential source files in New York, Miami, Los Angeles, Phoenix, Houston, and Chicago, we reviewed 1,332 payments for reimbursements of expenses to determine if they were supported with receipts. The results, as shown in the following table, illustrate that receipts were rarely provided for reimbursement payments.

Review of Reimbursements and Receipts				
Reimbursement Time frame	Number of Payments Reviewed	Total Amount of Reimbursements Reviewed	Receipts Attached	Percentage of Payments with Receipts
Prior to September 10, 1998	338	\$ 568,490	4	1%
September 10, 1998 through June 27, 2001	624	419,750	4	1%
After June 27, 2001	<u>370</u>	<u>241,579</u>	<u>30</u>	8%
	<u>1,332</u>	<u>\$1,229,819</u>	<u>38</u>	3%

Source: Office of the Inspector General Review of confidential source files.

Although the DEA did not require receipts to support reimbursement payments for 338 payments that occurred prior to September 1998, only 34 of the 994 (3 percent) reimbursement payments after that date that required receipts were properly supported. In addition, none of the 960 payments without receipts (\$638,278) made on or after September 10, 1998, contained an explanation as to why a receipt was not obtained.

When reviewing reimbursement payments, we examined the description noted in the remarks field of the DEA 103. We found that 775 of 1,332 reimbursement payments either had no description of the expenditure or generic descriptions such as "expenses incurred" or "U/C expenses." We believe it is important that the expense description be specific given the wide latitude agents have in

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

determining the amounts of the payments and the confidential nature of the transactions. The lack of receipts and the inadequate descriptions of the expenses create a lax internal control environment where payments may be approved that are not reasonable, appropriate, or justified. Consequently, we believe that DEA supervisors need to improve their oversight over reimbursements.

Approvals. The DEA Agent Manual requires that a second-line supervisor or above approve payments greater than \$2,500 and a Senior Executive Service-level manager and the designated Headquarters personnel from either the Office of Domestic Operations or the Office of International Operations approve payments greater than \$25,000. According to the Unit Chief of the Confidential Source Unit, a Receipt for Cash or Other Items (DEA 12) should be attached to the DEA 103 if the required supervisor approval of the payment is on the DEA 12. However, the DEA Agent Manual does not require the DEA 12 to be in the confidential source file.

During our audit work in New York and Miami, we noted that the DEA 12 forms generally were not found in the confidential source files. Therefore, in Los Angeles, Houston, Phoenix, and Chicago, we expanded our testing by requesting the DEA 12s if they were not found in the confidential source file. In Los Angeles, Phoenix, Houston, and Chicago, we reviewed 4,097 payments, of which 439 exceeded \$2,500 and consequently required approval beyond the agent's group supervisor. For 66 of the 439 payments (15 percent) totaling \$1,016,921, the DEA 103 did not reflect the appropriate supervisory approval and the division offices could not locate the DEA 12s to demonstrate appropriate supervisory approval. Without the higher-level manager's approval on or attached to the DEA 103, the document is incomplete and it is unclear whether the appropriate supervisor approved the payment.

Signatures. The DEA Agent Manual requires the confidential source to sign the establishing office's copy of the DEA 103 acknowledging that he/she has received the specified amount of money on a particular date. The agent that makes the payment (payer), the claimant (agent who requested the funds from the imprest fund), and a witness (another law enforcement officer) must sign the "receipt" as well. Once the payment is made and the DEA 103 is completed, the appropriate level of management signs the form.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

As part of our audit, we reviewed the DEA 103 to determine if:

- 1) all required signatures were documented on the form,
- 2) the confidential source signature appeared to be consistent among payments,
- 3) the witness or supervisor signature was a carbon, and
- 4) whether the DEA used "white out" for corrections rather than initialing the correction.

We generally observed that the payments had all the required signatures, the signatures appeared authentic, the witness and supervisor signatures were carbon copies, and corrections, if any, were crossed out and initialed.⁴¹ As shown in the following table, we only noted 91 out of 4,861 payments (about 2 percent) totaling \$331,355 that we observed issues with signatures.

Observed Issues with Signatures on DEA 103s

Issue	Number of payments
Missing payer signature (a)	7
Missing witness signature (a)	14
Missing supervisor signature (a)	13
Questionable confidential source signature (b)	18
Original rather than carbon signature (c)	39
Total	91

Source: Office of the Inspector General review of confidential source files.

- a. One explanation we were provided concerning the missing signatures was that the signature did not go through all the carbons. Based on the review of the documents in the confidential source file, we could not determine if the signatures were originally on the document.
- b. When reviewing the confidential source signature, we compared signatures among the payments in the file. In 18 instances, we observed confidential source's signatures that were not consistent with the source's signature on other payments. When we asked DEA officials about the questionable signatures, they indicated it was the confidential source signature and the variation could be due to the source signing the receipt in unusual circumstances such as on the hood of a car.
- c. Original signatures on the last page of a carbon form could indicate either the signature was not originally on the document but rather added after the DEA 103 was distributed, or the signature did not go through all the carbons and the final page was re-signed. Based on our review of the documents, we could not determine which occurred in these cases.

⁴¹ We observed the use of "white out" on 23 original payment documents. The use of white out obscures the information that is being corrected. The practice of crossing out the error and initialing the correction is the generally accepted method of correcting original documents because it does not obscure the information being corrected.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

During our testing, we also noted that 47 of 150 confidential source files we reviewed had signature exemplars for the confidential source.⁴² We discussed the issue of signature exemplars with DEA officials in Los Angeles and were told that they are no longer required. None of the four DEA Agent Manuals in effect since 1987 indicate that signature exemplars are required. However, the signature exemplars made it easier for a reviewer to validate the confidential source's signature, and we believe signature exemplars represent an additional internal control and best practice that should be reinstituted.

Miscellaneous issues. In reviewing the 150 confidential source files, we also noted other payment-related issues of concern. In most cases, the payments involved were either small dollar payments or the situation was an isolated instance. However, we discuss them briefly below because they relate to oversight of confidential source payments.

- We observed a total of 17 payments for \$52,240 (Houston and Miami) that note the payments were made to sources for sub-sources. The DEA Agent Manual indicates any individual who is paid by the DEA must be established as a confidential source. Therefore, it appears that the practice of paying sources to pay sub-sources conflicts that the DEA Agent Manual.
- In reviewing one file, we noted a letter indicating a DEA office made a substantial payment (\$19,900) from the asset forfeiture fund to a confidential source. The confidential source had been deactivated and deemed unsatisfactory months earlier. According to the DEA Agent Manual, a confidential source declared unsatisfactory will generally not be considered for award or monetary compensation. We found no documentation explaining why the source was being paid despite having been declared unsatisfactory. The Confidential Source Coordinator stated that the payment should not have been made.
- We noted four payments totaling \$7,150 in which the witness and supervisor was the same person. When we questioned

⁴² Signature exemplars are documents that provide samples of an individual's written signature. The signature exemplars would aid in verifying the confidential source's signature on payments. We observed signature exemplars in Phoenix (6 of 30), Washington (16 of 16), and Chicago (25 of 25) confidential source files.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

this, we were told that the DEA Agent Manual does not forbid this practice.

- An asset forfeiture award payment for \$1.25 million was recorded in the Miami Division. We observed the required Headquarters approval but were unable to verify the required division SES-level approval on the DEA 103. When we commented on the size of the payment, a Miami Associate Special Agent in Charge stated that such an award was commonplace and necessary given the danger faced and the scope of work these confidential source "employees" provide.
- Before a Defendant Use confidential source was officially established, a payment of \$4,000 was made to the source for information/services. According to the DEA Agent Manual, any confidential source that is paid by the DEA must be established. The Report of Investigation (DEA 6) explained that the \$4,000 payment was provided to the confidential source to help pay off a \$6,000 prior drug debt, although the source contributed \$2,000 of his/her own money. Generally, Defendant Use confidential sources do not receive information payments or awards. Further, the payment was made in July 2002, but the agent and supervisor did not sign the supporting DEA 6 until May 2003.

Recommendations

We recommend that the DEA:

4. Specifically identify what types of payments are to confidential sources and consistently identify those payments in the Federal Financial System. The DEA should pay specific attention to Budget Object Code 2533 - Payments to Foreign Police Officials and resolve an inconsistency between the Confidential Source Unit and the Office of Finance as to whether payments using Budget Object Code 2533 are confidential source payments.
5. Document the payment process for payments using non-appropriated funds (specifically High Intensity Drug Trafficking Areas) and develop an automated method to track these payments.
6. Account for all payments made to a confidential source by the DEA, not just payments using DEA-appropriated funds.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

7. Implement a formal process to reconcile all payments to confidential sources, both from appropriated and non-appropriated funds, to the Federal Financial System, the CSS Dollar database, and any other medium used to account for non-appropriated fund payments, such as HIDTA Imprest funds. This process should clearly identify who is responsible for the reconciliation, the time period the reconciliation should cover, and who approves the completed reconciliation.
8. Enhance controls over confidential source payments to prevent a deactivated confidential source or administratively closed case from being used to obligate or expend funds.
9. Develop a plan to correct the CSS Dollar database to reflect accurate, up-to-date data on confidential source payments and implement an audit trail to identify what changes were made to the electronic records. Alternatively, the DEA should develop another electronic process for monitoring calendar year and lifetime payments to confidential sources. If the DEA develops another electronic process, the DEA Agent Manual should be amended to reflect this new process.
10. Reinforce guidance to agents on the requirements of completing a Voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103). The reinforcement should address all sections of a complete DEA 103 including purpose of payment, remarks, signatures, and fund citation, as well as obtaining receipts when possible or documenting why a receipt is not possible.
11. Amend the DEA Agent Manual to require that Receipts for Cash or Other Items (DEA 12) be attached to DEA 103 if the DEA 12 is used to document the appropriate manager-level approval.
12. Consider reinstituting a requirement to obtain signature exemplars for confidential sources.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

STATEMENT ON THE INTERNAL CONTROLS

In planning and performing the audit of the DEA's Payments to Confidential Sources, we considered the DEA's internal control structure for the payments to those sources. We focused on the internal controls related to the determination of the amounts and types of payments made to individuals; the eligibility criteria and methodology for determining the amounts paid; and assessing the DEA's compliance with regulations concerning individuals who provide information for payment and controls over disbursements.

This evaluation was not made for the purpose of providing assurance on the DEA's internal controls over confidential source payments as a whole. However, we noted certain matters involving the internal controls that we considered to be reportable conditions under the *Government Auditing Standards*. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the ability of DEA to use funds efficiently and effectively. We found there was a lack of written documentation in the risk assessment process and that the DEA does not have an effective system to monitor payments to confidential sources (Findings I and II).

Because we are not expressing an opinion on DEA's controls over confidential source payments as a whole, this statement is intended solely for the information and use of DEA management in monitoring the Confidential Source Program. This restriction is not intended to further limit the distribution of this report.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of the audit were to assess the DEA's compliance with regulations concerning individuals who provide information for payment and controls over disbursements. We conducted our audit in accordance with the *Government Auditing Standards* and included such tests as were considered necessary to accomplish our objectives. Our audit concentrated on, but was not limited to, FYs 2001-2003.

Using confidential source payment information supplied by the Federal Financial System, we selected for file review judgmental samples of confidential sources who, during the period, received a significant amount of dollars, a significant number of payments, and few payments or dollars. We did not perform testing to express an opinion on the Federal Financial System, and therefore we do not express an opinion on it. However, as a part of the annual financial statement audit, the DEA financial management systems are reviewed to determine their compliance with the federal financial management systems requirements, applicable federal accounting standards, and the United States General Ledger. These systems were found to comply with these requirements for the FY 2003 financial statement audit. Therefore, we believe that the data used for our sampling and testing purposes was reliable to the extent needed.

As part of our review of the DEA Confidential Source Program we examined pertinent documents, including the four versions of the DEA Agent Manual in effect during our audit period; the DEA Financial Handbook, undated (obtained from the DEA in May 2003); and the Attorney General Guidelines Regarding the Use of Confidential Informants dated January 8, 2001, and May 30, 2002. We reviewed the DEA's process of establishing, paying, and monitoring confidential sources by reviewing 150 confidential source files, and we considered the impact of utilizing the confidential source by reviewing 64 closed case files. We conducted interviews of agents and finance personnel in headquarters and seven division offices. We performed our fieldwork at the Arlington, Virginia, Headquarters office of the DEA and in Washington, New York, Miami, Los Angeles, Phoenix, Houston, and Chicago division offices. In all cases, our samples were judgmentally selected.

The DEA supplied an extract of the Federal Financial System for confidential source payments. We summarized the payments by

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

division as the basis for selecting our sample of confidential source files to review. Initially, we reviewed 16 confidential source files in Washington and 12 confidential source files in Miami and New York. Of all the DEA Divisions, Miami and New York paid the most money to confidential sources in FY 2001-2002. We then reviewed 25 confidential source files in Chicago and Houston, and 30 confidential source files in Los Angeles and Phoenix. In selecting the additional sites, we considered amounts paid in total and the geographic region of office locations to obtain a cross-section of DEA offices in the audit. The sites visited comprised 63 percent of all the money paid to confidential sources in DEA domestic Divisions in FY 2001-2002.

We organized the selected divisions' payments into three categories:

- Confidential sources that received the most dollars during the period;
- Confidential sources that received the greatest number of payments in the period; and
- Confidential sources that received a few low dollar payments.

We selected a judgmental sample of confidential source files to review from the three categories, and reviewed all payments within the selected confidential source files.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

APPENDIX II

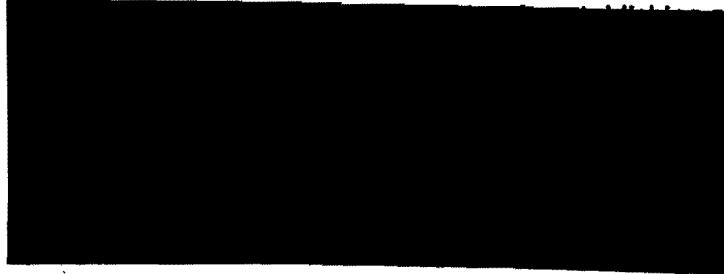
DEA FORMS

The following pages contain examples of each form listed below.

DEA 6 - Report of Investigation

The DEA 6 has varied uses. The form is intended for documentation of meetings, reviews, or actions taken by the DEA. In this audit, we observed the DEA 6 used for quarterly management reviews, debriefings, deactivations, and case initiation and closure.

DEA 512 - Confidential Source Establishment



B(7)(E)

DEA 473 - Confidential Source Agreement



B(7)(E)

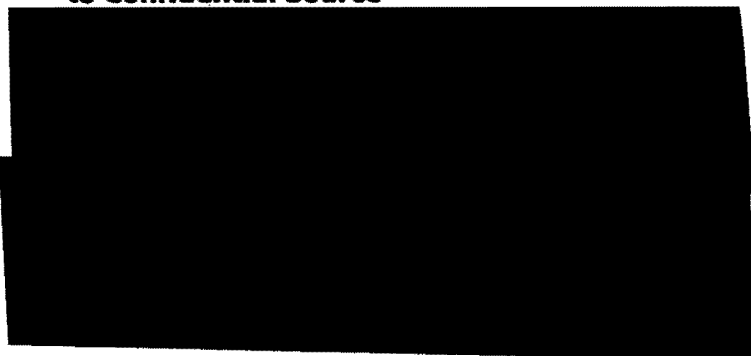
LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

DEA 12 - Receipt for Cash or other Items

A DEA 12 is the form used to identify money issued from the imprest fund for an advance other than travel. The DEA 12 is properly completed when it designates the person receiving the advance, file number, Geographic Drug Enforcement Program identifier, amount, Federal Financial System obligation document number, description, and purpose.

DEA 103 - Voucher for Purchase of Evidence or Payment to Confidential Source



B(7)(E)

DEA 356 - Informant Payment Record



LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

U.S. Department of Justice
Drug Enforcement Administration

REPORT OF INVESTIGATION (Continuation)	1. File No.	2. ASEP Identifier
	3. File Title	
4. Page 2 of 1		
5. Program Code	6. Date Presented	

DEA Form 100-100
JAN. 1970

CONFIDENTIAL
Drug Enforcement Administration

This report contains information which is confidential and its disclosure to the public would be injurious to the national defense.
It is to be controlled and its distribution limited to those personnel who have a valid need to know.
Previous editions of this form may be used.

DEA 12

FOR PLANS, TIES, AND/OR SPECIALTIES SEE OTHERS & APPLICATIONS

FILE NO.

GROUP 2: 1990-1999

FILM TYPE

DATE _____

DISPATCH CENTER OFFICE

A further observation regarding the following classified matter shall remain classified until such time as the information is declassified and released.

[illegible]

2000-01-01

NAME AND TITLE: _____

1949-1950

NAME AND TITLE OF DONOR

FOR RELEASE BY THE FBI

1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 26

- 60 -

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

8. the risk that the person might adversely affect a present or potential investigation or prosecution;
9. the extent the person's information or assistance can be corroborated;
10. the person's reliability and truthfulness;
11. the person's prior record as a witness in any proceeding;
12. whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution;
13. whether the person is reasonably believed to pose a danger to the public or other criminal threat, or is reasonably believed to pose a risk of flight;
14. whether the person is a substance abuser or has a history of substance abuse;
15. whether the person is a relative of an employee of any law enforcement agency;
16. the risk of physical harm that may occur to the person or his or her immediate family or close associates as a result of providing information or assistance to the Justice law enforcement agency; and
17. the record of the Justice law enforcement agency and the record of any other law enforcement agency (if available to the Justice law enforcement agency) regarding the person's prior or current service as a confidential source, Cooperating Defendant/Witness, or Source of Information, including, but not limited to, any information regarding whether the person was at any time terminated for cause.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

APPENDIX VIII

THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS

Preamble

The following Guidelines regarding the use of confidential informants are issued under the authority of the Attorney General as provided in sections 509, 510, and 533 of title 28, United States Code. They apply to the use of confidential informants in criminal investigations and prosecutions by Department of Justice law enforcement agencies and federal prosecuting offices as specified in paragraph (I)(A) below.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

TABLE OF CONTENTS

I. GENERAL PROVISIONS	1
A. PURPOSE AND SCOPE	1
B. DEFINITIONS	1
1. "Department of Justice Law Enforcement Agency" or "JLEA"	1
2. "Field Manager"	2
3. "Senior Field Manager"	2
4. "Federal Prosecuting Office" or "FPO"	2
5. "Chief Federal Prosecutor"	2
6. "Confidential Informant" or "CI"	2
7. "Cooperating Defendant/Witness"	2
8. "Source of Information"	3
9. "High Level Confidential Informant"	3
10. "Tier 1 Otherwise Illegal Activity"	3
11. "Tier 2 Otherwise Illegal Activity"	4
12. "Fugitive"	4
13. "Confidential Informant Review Committee" or "CIRC"	4
C. PROHIBITION ON COMMITMENTS OF IMMUNITY BY FEDERAL LAW ENFORCEMENT AGENCIES	5
D. REVEALING A CONFIDENTIAL INFORMANT'S TRUE IDENTITY	5
E. DUTY OF CANDOR	5
F. MAINTAINING CONFIDENTIALITY	5

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

G.	EXCEPTIONS AND DISPUTE RESOLUTION	7
H.	RIGHTS OF THIRD PARTIES	7
I.	COMPLIANCE	7
II.	REGISTERING A CONFIDENTIAL INFORMANT	8
A.	SUITABILITY DETERMINATION	8
1.	Initial Suitability Determination	8
2.	Continuing Suitability Review	9
3.	Review of Long-Term Confidential Informants	10
B.	REGISTRATION	11
C.	INSTRUCTIONS	11
D.	SPECIAL APPROVAL REQUIREMENTS	13
1.	High Level Confidential Informants	13
2.	Individuals Under the Obligation of a Legal Privilege of Confidentiality or Affiliated with the Media	14
3.	Federal Prisoners, Probationers, Parolees, Detainees, and Supervised Releasees	14
4.	Current or Former Participants in the Witness Security Program	15
5.	State or Local Prisoners, Probationers, Parolees, or Supervised Releasees	15
6.	Fugitives	16
III.	RESPONSIBILITIES REGARDING REGISTERED CONFIDENTIAL INFORMANTS	17
A.	GENERAL PROVISIONS	17
1.	No Interference With an Investigation of a Confidential Informant	17

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

2.	Prohibited Transactions and Relationships	17
B.	MONETARY PAYMENTS	17
1.	General	17
2.	Prohibition Against Contingent Payments	18
3.	Approval for a Single Payment	18
4.	Approval for Annual Payments	18
5.	Approval for Aggregate Payments	18
6.	Documentation of Payment	18
7.	Accounting and Reconciliation Procedures	19
8.	Coordination with Prosecution	19
C.	AUTHORIZATION OF OTHERWISE ILLEGAL ACTIVITY	19
1.	General Provisions	19
2.	Authorization	20
3.	Findings	20
4.	Instructions	21
5.	Precautionary Measures	22
6.	Suspension of Authorization	23
7.	Revocation of Authorization	23
8.	Renewal and Expansion of Authorization	23
9.	Emergency Authorization	24
10.	Designees	24

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

D.	LISTING A CONFIDENTIAL INFORMANT IN AN ELECTRONIC SURVEILLANCE APPLICATION	24
IV.	SPECIAL NOTIFICATION REQUIREMENTS	25
A.	NOTIFICATION OF INVESTIGATION OR PROSECUTION	25
B.	NOTIFICATION OF UNAUTHORIZED ILLEGAL ACTIVITY	25
C.	NOTIFICATION REGARDING CERTAIN FEDERAL JUDICIAL PROCEEDINGS	26
D.	PRIVILEGED OR EXCULPATORY INFORMATION	26
E.	RESPONDING TO REQUESTS FROM CHIEF FEDERAL PROSECUTORS REGARDING A CONFIDENTIAL INFORMANT	27
F.	FILE REVIEWS	27
G.	DESIGNERS	27
V.	DEACTIVATION OF CONFIDENTIAL INFORMANTS	27
A.	GENERAL PROVISIONS	27
B.	DELAYED NOTIFICATION TO A CONFIDENTIAL INFORMANT	28
C.	CONTACTS WITH FORMER CONFIDENTIAL INFORMANTS DEACTIVATED FOR CAUSE	28
D.	COORDINATION WITH PROSECUTORS	28

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

I. GENERAL PROVISIONS

A. PURPOSE AND SCOPE

1. The purpose of these Guidelines is to set policy regarding the use of Confidential Informants, as defined below, in criminal investigations and prosecutions by all Department of Justice Law Enforcement Agencies and Federal Prosecuting Offices, as defined below.
2. These Guidelines do not apply to the use of Cooperating Defendants/Witnesses or Sources of Information, as defined below, unless a Department of Justice Law Enforcement Agency, in its discretion, chooses to apply these Guidelines to such persons.
3. These Guidelines are mandatory and supersede the Attorney General's Guidelines on the Use of Informants in Domestic Security, Organized Crime, and Other Criminal Investigations (December 15, 1976); the Attorney General's Guidelines on FBI Use of Informants and Confidential Sources (December 2, 1980); Resolution 18 of the Office of Investigative Agency Policies (August 15, 1996); and any other guidelines or policies that are inconsistent with these Guidelines. These Guidelines do not supersede otherwise applicable ethical obligations of Department of Justice attorneys, which can, in certain circumstances (for example, with respect to contacts with represented persons), have an impact on law enforcement agents' conduct.
4. These Guidelines do not limit the ability of a Department of Justice Law Enforcement Agency to impose additional restrictions on the use of Confidential Informants.
5. These Guidelines apply to the use of a Confidential Informant in a foreign country only to the extent that the Confidential Informant is reasonably likely to be called to testify in a domestic case.
6. These Guidelines do not apply to the use of Confidential Informants in foreign intelligence or foreign counterintelligence investigations.

B. DEFINITIONS

1. "Department of Justice Law Enforcement Agency" or "JLEA":
 - a. The Drug Enforcement Administration;
 - b. The Federal Bureau of Investigation;
 - c. The Immigration and Naturalization Service;

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- d. The United States Marshals Service; and
- e. The Department of Justice Office of the Inspector General.
- 2. "Field Manager" - a JLEA's first-line supervisor, as defined by the JLEA (typically, GS-14 rank or higher).
- 3. "Senior Field Manager" - a JLEA's second-line supervisor, as defined by the JLEA (typically, GS-15 rank or higher).
- 4. "Federal Prosecuting Office" or "FPO" -
 - a. The United States Attorneys' Offices;
 - b. The Criminal Division, Tax Division, Civil Rights Division, Antitrust Division, and Environmental and Natural Resources Division of the Department of Justice; and
 - c. Any other litigating component of the Department of Justice with authority to prosecute federal criminal offenses.
- 5. "Chief Federal Prosecutor" - the head of a FPO.
- 6. "Confidential Informant" or "CI" - any individual who provides useful and credible information to a JLEA regarding felonious criminal activities, and from whom the JLEA expects or intends to obtain additional useful and credible information regarding such activities in the future.
- 7. "Cooperating Defendant/Witness" - any individual who:
 - a. meets the definition of a CI;
 - b. has agreed to testify in a proceeding as a result of having provided information to the JLEA; and
 - c. (i) is a defendant or potential witness who has a written agreement with a FPO, pursuant to which the individual has an expectation of future judicial or prosecutive consideration or assistance as a result of having provided information to the JLEA, or
 - (ii) is a potential witness who has had a FPO concur in all material aspects of his or her use by the JLEA.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

8. "Source of Information" - any individual who:
 - a. meets the definition of a CI;
 - b. provides information to a JLEA solely as a result of legitimate routine access to information or records, such as an employee of the military, a law enforcement agency, or a legitimate business (e.g., phone company, banks, airlines), and not as a result of criminal association with persons of investigative interest to the JLEA; and
 - c. provides such information in a manner consistent with applicable law.
9. "High Level Confidential Informant" - a CI who is part of the senior leadership of an enterprise that
 - a. has: (i) a national or international sphere of activities, or (ii) high significance to the JLEA's national objectives, even if the enterprise's sphere of activities is local or regional; and
 - b. engages in, or uses others to commit, any of the conduct described below in paragraph (b)(10)(b)(i)-(iv).
10. "Tier 1 Otherwise Illegal Activity" - any activity that:
 - a. would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization; and
 - b. that involves -
 - (i) the commission, or the significant risk of the commission, of any act of violence by a person or persons other than the Confidential Informant;¹
 - (ii) corrupt conduct, or the significant risk of corrupt conduct, by senior federal, state, or local public officials;

¹ Bookmaking that is significantly associated with, or substantially controlled by, organized crime ordinarily will be within the scope of paragraph (b)(10)(b)(i). Thus, for example, those bookmakers have a financial relationship with members or associates of organized crime, and/or use members or associates of organized crime to collect their debts; the conduct of those bookmakers would create a significant risk of violence, and would therefore fall within the definition of Tier 1 Otherwise Illegal Activity.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

(iii) the manufacturing, importing, exporting, possession, or trafficking of controlled substances in a quantity equal to or exceeding those quantities specified in United States Sentencing Guidelines § 2D1.1(c)(1);

(iv) financial loss, or the significant risk of financial loss, in an amount equal to or exceeding those amounts specified in United States Sentencing Guidelines § 2B1.1(b)(1)(I);²

(v) a Confidential Informant providing to any person (other than a JLEA agent) any item, service, or expertise that is necessary for the commission of a federal, state, or local offense, which the person otherwise would have difficulty obtaining; or

(vi) a Confidential Informant providing to any person (other than a JLEA agent) any quantity of a controlled substance, with little or no expectation of its recovery by the JLEA.

11. "Tier 2 Otherwise Illegal Activity" - any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.
12. "Fugitive" - an individual:
 - a. for whom a federal, state, or local law enforcement agency has placed a wanted record in the NCIC (other than for a traffic or petty offense);
 - b. who is located either within the United States or in a country with which the United States has an extradition treaty; and

The citations to the United States Sentencing Guidelines (USSG) Manual are to the 2001 Edition. The references herein to particular USSG Sections are intended to remain applicable to the most closely corresponding USSG level in subsequent editions of the USSG Manual in the event that the cited USSG provisions are amended. Thus, it is intended that subsection (iii) of this paragraph will remain applicable to the highest offense level in the Drug Quantity Table in future editions of the USSG Manual, and that subsection (iv) of the paragraph will remain applicable to dollar amounts that, in future editions of the USSG Manual, trigger sentencing enhancements similar to that set forth in the current Section 2B1.1(b)(1)(I). Any ambiguities in this regard should be resolved by the Assistant Attorney General for the Criminal Division.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- c. whom the law enforcement agency that has placed the wanted record in the NCIC is willing to take into custody upon his or her arrest and, if necessary, seek his or her extradition to its jurisdiction.
- 13. "Confidential Informant Review Committee" or "CIRC" - a committee, created by a JLEA for purposes of reviewing certain decisions relating to the registration and utilization of CIs, the chair of which is a JLEA official at or above the level of Deputy Assistant Director (or its equivalent) and the membership of which includes the following two representatives designated by the Assistant Attorney General for the Criminal Division of the Department of Justice (each of whom shall be considered a "Criminal Division representative"): (i) a Deputy Assistant Attorney General for the Criminal Division; and (ii) an Assistant United States Attorney.

C. PROHIBITION ON COMMITMENTS OF IMMUNITY BY FEDERAL LAW ENFORCEMENT AGENCIES

A JLEA agent does not have any authority to make any promise or commitment that would prevent the government from prosecuting an individual for criminal activity that is not authorized pursuant to paragraph (III)(C) below, or that would limit the use of any evidence by the government, without the prior written approval of the FPO that has primary jurisdiction to prosecute the CI for such criminal activity. A JLEA agent must take the utmost care to avoid giving any person the erroneous impression that he or she has any such authority.

D. REVEALING A CONFIDENTIAL INFORMANT'S TRUE IDENTITY

Except in the case of approvals and reviews described below in paragraphs (II)(A)(3) (review of long-term CIs), (III)(B)(8) (coordination concerning payments to CIs), (IV)(D)(1) (notification that CI has obtained privileged information), and (V)(D) (coordination concerning deactivation of CI, but only with respect to a CI whose identity was not previously disclosed), whenever a JLEA is required to make contact of any kind with a FPO pursuant to these Guidelines regarding a CI, the JLEA may not withhold the true identity of the CI from the FPO.

E. DUTY OF CANDOR

Employees of the entities to which these Guidelines apply have a duty of candor in the discharge of their responsibilities pursuant to these Guidelines.

F. MAINTAINING CONFIDENTIALITY

- 1. A JLEA agent must take the utmost care to avoid conveying any confidential investigative information to a CI (e.g., information relating to legitimate

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

surveillance, search warrants, or the identity of other actual or potential informants), other than what is necessary and appropriate for operational reasons.

2. The Chief Federal Prosecutor and his or her designee are required to maintain as confidential the identity of any CI and the information the CI has provided, unless obligated to disclose it by law or Court order. If a JLEA provides the Chief Federal Prosecutor or his or her designee with written material containing such information:
 - a. Such individual is obligated to keep it confidential by placing it into a locked file cabinet when not in his or her direct care and custody;
 - b. Access to the information shall be restricted to the Chief Federal Prosecutor or his or her designee and personnel deemed necessary to carry out the official duties related to the case;
 - c. The Chief Federal Prosecutor or his or her designee is responsible for assuring that each person permitted access to the information is made aware of the need to preserve the security and confidentiality of the information, as provided in this policy;
 - d. Prior to disclosure of the information to defense counsel or in open Court, the Chief Federal Prosecutor or his or her designee must give the JLEA an opportunity to discuss such disclosure and must comply with any other applicable provision of 28 C.F.R. §§ 16.21-16.29; and
 - e. At the conclusion of a case or investigation, all written materials containing the information that have not been disclosed shall be forwarded to the JLEA that provided them.³
3. Employees of a JLEA and employees of a FPO have a continuing obligation after leaving employment with the Department of Justice and its constituent components to maintain as confidential the identity of any CI and the information he or she provided, unless the employee is obligated to disclose it by law or Court order. See 28 C.F.R. §§ 16.21-16.29.

³ This requirement shall not prevent the Chief Federal Prosecutor or his or her designee from keeping in the relevant case file materials such as motions, responses, legal memoranda, Court orders, and internal office memoranda and correspondence. If any such materials contain information revealing a CI's true identity, the Chief Federal Prosecutor or his or her designee shall maintain the materials in accordance with the provisions of paragraph 1(F)(2)(c)(d) above.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

G. EXCEPTIONS AND DISPUTE RESOLUTION

1. Whenever any of the entities to which these Guidelines apply believes that an exception to any provision of these Guidelines is justified, or whenever there is a dispute between or among any such entities (other than a dispute with the Criminal Division of the Department of Justice) regarding these Guidelines, an exception must be sought from, or the dispute shall be resolved by, the Assistant Attorney General (AAG) for the Criminal Division or his or her designee. The Deputy Attorney General or his or her designee shall hear appeals, if any, from decisions of the AAG.
2. Whenever there is a dispute between the Criminal Division and any of the other entities to which these Guidelines apply, such dispute shall be resolved by the Deputy Attorney General or his or her designee.
3. Any exception granted or dispute resolved pursuant to this paragraph shall be documented in the JLEA's files.

H. RIGHTS OF THIRD PARTIES

Nothing in these Guidelines is intended to create or does create an enforceable legal right or private right of action by a CI or any other person.

I. COMPLIANCE

1. Within 120 days of the approval of these Guidelines by the Attorney General, each JLEA shall develop agency-specific guidelines that comply with these Guidelines, and submit such agency-specific guidelines to the AAG for the Criminal Division for review. The agency-specific guidelines must ensure, at a minimum, that the JLEA's agents receive sufficient initial and in-service training in the use of CIs consistent with these Guidelines, and that compliance with these Guidelines is considered in the annual performance appraisal of its agents. As part of such compliance the JLEA shall designate a senior official to oversee all aspects of its CI program, including the training of agents, registration, review, and termination of CIs, and notifications to outside entities.
2. Within 30 days of the approval of these Guidelines, each JLEA shall establish a Confidential Informant Review Committee (CIRC) for the purpose of conducting the review procedures specified in paragraphs (II)(A)(3), (II)(D)(1), and (II)(D)(2).

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

II. REGISTERING A CONFIDENTIAL INFORMANT

A. SUITABILITY DETERMINATION

1. Initial Suitability Determination

Prior to utilizing a person as a CI, a case agent of a JLEA shall complete and sign a written Initial Suitability Report and Recommendation, which shall be forwarded to a Field Manager for his or her written approval. In completing the Initial Suitability Report and Recommendation, the case agent must address the following factors (or indicate that a particular factor is not applicable):

- a. the person's age;
- b. the person's alien status;
- c. whether the person is a public official, law enforcement officer, union official, employee of a financial institution or school, member of the military services, a representative or affiliate of the media, or a party to, or in a position to be a party to, privileged communications (e.g., a member of the clergy, a physician, or a lawyer);
- d. the extent to which the person would make use of his or her affiliations with legitimate organizations in order to provide information or assistance to the JLEA, and the ability of the JLEA to ensure that the person's information or assistance is limited to criminal matters;
- e. the extent to which the person's information or assistance would be relevant to a present or potential investigation or prosecution and the importance of such investigation or prosecution;
- f. the nature of any relationship between the CI and the subject or target of an existing or potential investigation or prosecution, including but not limited to a current or former spousal relationship or other family tie, and any current or former employment or financial relationship;
- g. the person's motivation in providing information or assistance, including any consideration sought from the government for this assistance;
- h. the risk that the person might adversely affect a present or potential investigation or prosecution.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- i. the extent to which the person's information or assistance can be corroborated;
- j. the person's reliability and truthfulness;
- k. the person's prior record as a witness in any proceeding;
- l. whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution;
- m. whether the person is reasonably believed to pose a danger to the public or other criminal threat, or is reasonably believed to pose a risk of flight;
- n. whether the person is a substance abuser or has a history of substance abuse;
- o. whether the person is a relative of an employee of any law enforcement agency;
- p. the risk of physical harm that may occur to the person or his or her immediate family or close associates as a result of providing information or assistance to the JLEA; and
- q. the record of the JLEA and the record of any other law enforcement agency (if available to the JLEA) regarding the person's prior or current service as a CI, Cooperating Defendant/Witness, or Source of Information, including, but not limited to, any information regarding whether the person was at any time terminated for cause.

2. Continuing Suitability Review

- a. Each CP's file shall be reviewed by the case agent at least annually. The case agent shall complete and sign a written Continuing Suitability Report and Recommendation, which shall be forwarded to a Field Manager for his or her written approval. In completing the Continuing Suitability Report and Recommendation, the case agent must address the factors set forth above in paragraph (II)(A)(1) (or indicate that a particular factor is not applicable) and, in addition, the length of time that the individual has been registered as a CI and the length of time that the individual has been handled by the same agent or agents.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- b. Each JLEA shall establish systems to ensure that all available information that might materially alter a prior suitability determination, including, but not limited to, information pertaining to unauthorized illegal activity by the CI, is promptly reported to a Field Manager and then recorded and maintained in the CI's file. See (IV)(B)(2) below. Upon receipt of any such information, the Field Manager shall ensure that a new Continuing Suitability Report and Recommendation is promptly prepared in light of such new information.

3. Review of Long-Term Confidential Informants⁴

- a. When a CI has been registered for more than six consecutive years, and, to the extent such a CI remains open, every six years thereafter, the CIRC shall review the CI's completed Initial and Continuing Suitability Reports and Recommendations and decide whether, and under what conditions, the individual should continue to be utilized as a CI. A Criminal Division representative on the CIRC who disagrees with the decision to approve the continued use of such an individual as a Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).
- b. Every three years after a CI's file is reviewed pursuant to the provisions of paragraph (II)(A)(3)(a), if the CI remains registered, the JLEA shall conduct an internal review, including review by a designated senior headquarters official, of the CI's completed Initial and Continuing Suitability Reports and Recommendations. If the designated senior headquarters official decides that there are any apparent or potential problems that may warrant any change in the use of the CI, the official shall (i) consult the appropriate Senior Field Manager and (ii) provide the Initial and Continuing Suitability Reports and Recommendations to the CIRC for review in accord with paragraph (II)(A)(3)(a).

⁴ This provision did not apply until one year after these Guidelines' original effective date of January 8, 2001, when the first set of Continuing Suitability Reports and Recommendations was completed. Further, during the first three years that this provision is in effect, each CIRC may stagger the review of some long-term CIs in order to even out the number of files that must initially be reviewed. However, no later than four years after the original effective date of these Guidelines, all of the CIs who were registered for more than six consecutive years as of the original effective date of these Guidelines must be reviewed pursuant to this provision.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

B. REGISTRATION

After a Field Manager has approved an individual as suitable to be a CI, the individual shall be registered with that JLEA as a CI. In registering a CI, the JLEA shall, at a minimum, document or include the following in the CI's files:

1. a photograph of the CI;
2. the JLEA's efforts to establish the CI's true identity;
3. the results of a criminal history check for the CI;
4. the Initial Suitability Report and Recommendation;
5. any promises or benefits, and the terms of such promises or benefits, that are given a CI by a JLEA or any other law enforcement agency (if available to the JLEA);
6. any promises or benefits, and the terms of such promises or benefits, that are given a CI by any FPO or any state or local prosecuting office (if available to the JLEA); and
7. all information that is required to be documented in the CI's files pursuant to these Guidelines (e.g., the provision of the instructions set forth in the next paragraph).

C. INSTRUCTIONS

1. In registering a CI, at least one agent of the JLEA, along with one additional agent or other law enforcement official present as a witness, shall review with the CI written instructions that state that:
 - a. information provided by the CI to the JLEA must be truthful;
 - b. the CI's assistance and the information provided are entirely voluntary;
 - c. the United States Government will strive to protect the CI's identity but cannot guarantee that it will not be divulged;
 - d. [if applicable] the JLEA on its own cannot promise or agree to any immunity from prosecution or other consideration by a Federal Prosecutor's Office or a Court in exchange for the CI's cooperation, since the decision to confer any such benefit lies within the exclusive discretion

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

of the Federal Prosecutor's Office and the Court. However, the JLEA will consider (but not necessarily act upon) a request by the CI to advise the appropriate Federal Prosecutor's Office or Court of the nature and extent of his or her assistance to the JLEA;³

- a. [(if applicable)] the CI has not been authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity;⁴
- f. the CI must abide by the instructions of the JLEA and must not take or seek to take any independent action on behalf of the United States Government;
- g. the CI is not an employee of the United States Government and may not represent himself or herself as such;
- h. the CI may not enter into any contract or incur any obligation on behalf of the United States Government, except as specifically instructed and approved by the JLEA;
- i. the JLEA cannot guarantee any rewards, payments, or other compensation to the CI;
- j. in the event that the CI receives any rewards, payments, or other compensation from the JLEA, the CI is liable for any taxes that may be owed; and

³ This instruction should be provided if there is any apparent issue of criminal liability or penalties that relates to the CI. Whether or not this instruction is given to a CI, the JLEA does not have any authority to make any promise or commitment that would prevent the Government from prosecuting an individual, except as provided in paragraphs (I)(C) above and (III)(G) below, and a JLEA agent must avoid giving any person the erroneous impression that he or she has any such authority.

⁴ This instruction should be provided to any CI who is not authorized to engage in otherwise illegal activity. See paragraph (III)(C)(4) for instructions that must be provided to a CI who is, in fact, authorized to engage in otherwise illegal conduct.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- k. [if applicable] no promises or commitments can be made, except by the Immigration and Naturalization Service, regarding the alien status of any person or the right of any person to enter or remain in the United States.⁷
- 2. The content and meaning of each of the foregoing instructional points must be clearly conveyed to the CI. Immediately after these instructions have been given, the agent shall require the CI to acknowledge his or her receipt and understanding of the instructions. The agent and the other law enforcement official shall document that the instructions were reviewed with the CI and that the CI acknowledged the instructions and his or her understanding of them. As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the documentation.
- 3. The instruction and documentation procedures shall be repeated whenever it appears necessary or prudent to do so, and in any event at least every twelve months.

D. SPECIAL APPROVAL REQUIREMENTS

1. High Level Confidential Informants

- a. Prior to utilizing an individual as a High Level Confidential Informant, a case agent of a JLEA shall first obtain the written approval of the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision to approve the use of an individual as a High Level Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).
- b. In deciding whether to approve the use of a High Level Confidential Informant, the CIRC shall have access to any Initial or Completed Suitability Reports and Recommendations for the individual in question.
- c. After a final decision has been made to approve the use of a High Level Confidential Informant, the CIRC shall consider whether to notify the Chief Federal Prosecutor of any FPO that is participating in the conduct of an investigation that is, or would be, utilizing the High Level Confidential Informant, or any FPO that has been, or would be, working with that individual in connection with a prosecution, of this decision to approve that individual as a High Level Confidential Informant. If the CIRC determines that no such notification shall be made, the reason or reasons for the determination shall be provided to the Criminal Division.

⁷ This instruction should be provided if there is any separate issue of immigration status that relates to the CI and the JLEA is not the Immigration and Naturalization Service.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

representatives on the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision not to provide such notification may seek review of that decision pursuant to paragraph (I)(G).

2. Individuals Under the Obligation of a Legal Privilege of Confidentiality or Affiliated with the Media

- a. Prior to utilizing as a Confidential Informant an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media, a case agent of a JLEA shall first obtain the written approval of the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision to approve the use of such an individual as a Confidential Informant may seek review of that decision pursuant to paragraph (I)(G).
- b. In deciding whether to approve the use as a Confidential Informant of an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media, the CIRC shall have access to any Initial or Completed Suitability Reports and Recommendations for the individual in question.
- c. After a final decision has been made to approve the use of an individual who is under the obligation of a legal privilege of confidentiality or affiliated with the media as a Confidential Informant, the CIRC shall consider whether to notify the Chief Federal Prosecutor of any FPO that is participating in the conduct of an investigation that is, or would be, utilizing the individual, or any FPO that has been, or would be, working with that individual in connection with a prosecution, of the decision to approve that individual as a Confidential Informant. If the CIRC determines that no such notification shall be made, the reason or reasons for the determination shall be provided to the Criminal Division representatives on the CIRC. A Criminal Division representative on the CIRC who disagrees with a decision not to provide such notification may seek review of that decision pursuant to paragraph (I)(G).

3. Federal Prisoners, Probationers, Parolees, Detainees, and Supervised Releasees

- a. Consistent with current Department of Justice requirements, a JLEA must receive the approval of the Criminal Division's Office of Enforcement Operations ("OEO") prior to utilizing as a CI an individual who is in the custody of the United States Marshals Service or the Bureau of Prisons, or who is under Bureau of Prisons supervision. See U.S.A.M. § 9-21.040.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

b. Prior to utilizing a federal probationer, parolee, or supervised releasee as a CI, a Field Manager of a JLEA shall determine if the use of that person in such a capacity would violate the terms and conditions of the person's probation, parole, or supervised release. If the Field Manager has reason to believe that it would violate such terms and conditions, prior to using the person as a CI, the Field Manager or his or her designee must obtain the permission of a federal probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the CI's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate federal official, the JLEA may seek to obtain authorization for the use of such individual as a CI from the Court then responsible for the individual's probation, parole, or supervised release, provided that the JLEA first consults with the FPO for that District.

c. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a federal probationer, parolee, or supervised releasee would be utilized as a CI, or where a FPO would be working with a federal probationer, parolee, or supervised releasee in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

4. Current or Former Participants in the Witness Security Program

a. Consistent with extant Department of Justice requirements, a JLEA must receive the approval of OEO and the sponsoring prosecutor (or his or her successor) prior to utilizing as a CI a current or former participant in the Federal Witness Security Program, provided further that the OEO will coordinate such matters with the United States Marshals Service. See U.S.A.M. § 9-21.800.

b. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a current or former participant in the Witness Security Program would be utilized as a CI, or where a FPO would be working with a current or former participant in the Witness Security Program in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

5. State or Local Prisoners, Probationers, Parolees, or Supervised Releasees

a. Prior to utilizing a state or local prisoner, probationer, parolee, or supervised releasee as a CI, a Field Manager of a JLEA shall determine if the use of that person in such a capacity would violate the terms and

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

conditions of the person's incarceration, probation, parole, or supervised release. If the Field Manager has reason to believe that it would violate such terms and conditions, prior to using the person as a CI, the Field Manager or his or her designee must obtain the permission of a state or local prison, probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the CI's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate state or local official, the JLEA may seek to obtain authorization for the use of such individual as a CI from the state or local Court then responsible for the individual's incarceration, probation, parole, or supervised release.

- b. In situations where a FPO is either participating in the conduct of an investigation by a JLEA in which a state or local prisoner, probationer, parolee, or supervised releasee would be utilized as a CI, or where a FPO would be working with a state or local prisoner, probationer, parolee, or supervised releasee in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter prior to using the person as a CI.

6. Fugitives

- a. Except as provided below, a JLEA shall have no communication with a current or former CI who is a fugitive.
- b. A JLEA is permitted to have communication with a current or former CI who is a fugitive:
 - (i) if the communication is part of a legitimate effort by that JLEA to arrest the fugitive; or
 - (ii) if approved, in advance whenever possible, by a Senior Field Manager of any federal, state, or local law enforcement agency that has a wanted record for the individual in the NCIC and, in the case of a federal warrant, by the FPO for the issuing District.
- c. A JLEA that has communication with a fugitive must promptly report such communication to all federal, state, and local law enforcement agencies and other law enforcement agencies having a wanted record for the individual in the NCIC, and document those communications in the CI's files.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

**III. RESPONSIBILITIES REGARDING REGISTERED
CONFIDENTIAL INFORMANTS**

A. GENERAL PROVISIONS

1. No Interference With an Investigation of a Confidential Informant

A JLEA agent must take the utmost care to avoid interfering with or impeding any criminal investigation or arrest of a CI. No agent shall reveal to a CI any information relating to an investigation of the CI. An agent shall not confirm or deny the existence of any investigation of the CI, unless authorized to do so by the Chief Federal Prosecutor; nor shall an agent agree to a request from a CI to determine whether the CI is the subject of any investigation.

2. Prohibited Transactions and Relationships

- a. A JLEA agent shall not: (i) exchange gifts with a CI; (ii) provide the CI with any thing of more than nominal value; (iii) receive any thing of more than nominal value from a CI; or (iv) engage in any business or financial transactions with a CI. Except as authorized pursuant to paragraph (III)(B) below, any exception to this provision requires the written approval of a Field Manager, in advance whenever possible, based on a written finding by the Field Manager that the event or transaction in question is necessary and appropriate for operational reasons. This written finding shall be maintained in the CI's files.
- b. A Federal Law Enforcement agent shall not socialize with a CI except to the extent necessary and appropriate for operational reasons.
- c. In situations where a FFO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter, in advance whenever possible, if the JLEA approves an exception under paragraph (III)(A)(2)(a) or if a Federal Law Enforcement agent socializes with a CI in a manner not permitted under paragraph (III)(A)(2)(b).

B. MONETARY PAYMENTS

1. General

Monies that a JLEA pays to a CI in the form of fees and rewards shall be commensurate with the value, as determined by the JLEA, of the information he or she provided for the

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

assistance he or she rendered to that JLEA. A JLEA's reimbursement of expenses incurred by a CI shall be based upon actual expenses incurred.

2. Prohibition Against Contingent Payments

Under no circumstances shall any payments to a CI be contingent upon the conviction or punishment of any individual.

3. Approval for a Single Payment

A single payment of between \$2,500 and \$25,000 per case to a CI must be authorized, at a minimum, by a JLEA's Senior Field Manager. A single payment in excess of \$25,000 per case shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official.

4. Approval for Annual Payments

Consistent with paragraph (III)(B)(3) above, payments by a JLEA to a CI that exceed an aggregate of \$100,000 within a one-year period, as that period is defined by the JLEA, shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official. The headquarters official may authorize additional aggregate annual payments in increments of \$50,000 or less.

5. Approval for Aggregate Payments

Consistent with paragraphs (III)(B)(3)-(4), and regardless of the time frame, any payments by a JLEA to a CI that exceed an aggregate of \$200,000 shall be made only with the authorization of the Senior Field Manager and the express approval of a designated senior headquarters official. After the headquarters official has approved payments to a CI that exceed an aggregate of \$200,000, the headquarters official may authorize, subject to paragraph (III)(B)(4) above, additional aggregate payments in increments of \$100,000 or less.

6. Documentation of Payment

The payment of any monies to a CI shall be witnessed by at least two law enforcement representatives. Immediately after receiving a payment, the CI shall be required to sign or initial, and date, a written receipt.⁵ At the time of the payment, the representative shall advise the CI that the monies may be taxable income that must be reported to appropriate tax authorities. Thereafter, those representatives shall document the payment and the advice of taxability in the

⁵ The CI may sign or initial the written receipt by using a pseudonym which has been previously approved and documented in the CI's file and designated for use by only one CI.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

JLEA's files. The documentation of payment shall specify whether the payment is for information, services, or expenses.

7. Accounting and Reconciliation Procedures

Each JLEA shall establish accounting and reconciliation procedures to comply with these Guidelines. Among other things, these procedures shall reflect all monies paid to a CI subsequent to the issuance of these Guidelines.

8. Coordination with Prosecution

In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall coordinate with the attorney assigned to the matter, in advance whenever possible, the payment of monies to the CI pursuant to paragraphs (III)(B)(3)-(5) above.

C. AUTHORIZATION OF OTHERWISE ILLEGAL ACTIVITY

1. General Provisions

- a. A JLEA shall not authorize a CI to engage in any activity that otherwise would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization, except as provided in the authorization provisions in paragraph (III)(C)(2) below.
- b. A JLEA is never permitted to authorize a CI to:
 - (i) participate in an act of violence;
 - (ii) participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);
 - (iii) participate in an act designed to obtain information for the JLEA that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search); or
 - (iv) initiate or instigate a plan or strategy to commit a federal, state, or local offense.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

2. Authorization

- a. Tier 1 Otherwise Illegal Activity must be authorized in advance and in writing for a specified period, not to exceed 90 days, by:
 - (i) a JLEA's Special Agent in Charge (or the equivalent); and
 - (ii) the appropriate Chief Federal Prosecutor²
- b. Tier 2 Otherwise Illegal Activity must be authorized in advance and in writing for a specified period, not to exceed 90 days, by a JLEA's Senior Field Manager.
- c. For purposes of this paragraph, the "appropriate Chief Federal Prosecutor" is the Chief Federal Prosecutor that: (i) is participating in the conduct of an investigation by a JLEA that is utilizing that active CI, or is working with that active CI in connection with a prosecution; (ii) with respect to Otherwise Illegal Activity that would constitute a violation of federal law, would have primary jurisdiction to prosecute the Otherwise Illegal Activity; or (iii) with respect to Otherwise Illegal Activity that would constitute a violation only of state or local law, is located where the otherwise criminal activity is to occur.

3. Findings

- a. The JLEA official who authorizes Tier 1 or 2 Otherwise Illegal Activity must make a finding, which shall be documented in the CI's files, that authorization for the CI to engage in the Tier 1 or 2 Otherwise Illegal Activity is -
 - (i) necessary either to -
 - (A) obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization; or

² Even without an express act of Congress authorizing the conduct of such, it is within the power and the duty of federal prosecutors, as executive branch officers, to take reasonable measures to discharge the duties imposed on them as executive branch officers, and they will be immune from state action if they take such measures under color of federal law and in good faith.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

(B) prevent death, serious bodily injury, or significant damage to property; and

(ii) that in either case the benefits to be obtained from the CI's participation in the Tier 1 or 2 Otherwise Illegal Activity outweigh the risks.

b. In making these findings, the JLEA shall consider, among other things:

(i) the importance of the investigation;

(ii) the likelihood that the information or evidence sought will be obtained;

(iii) the risk that the CI might misunderstand or exceed the scope of his authorization;

(iv) the extent of the CI's participation in the Otherwise Illegal Activity;

(v) the risk that the JLEA will not be able to supervise closely the CI's participation in the Otherwise Illegal Activity;

(vi) the risk of violence, physical injury, property damage, and financial loss to the CI or others; and

(vii) the risk that the JLEA will not be able to ensure that the CI does not profit from his or her participation in the authorized Otherwise Illegal Activity.

4. Instructions

a. After a CI is authorized to engage in Tier 1 or 2 Otherwise Illegal Activity, at least one agent of the JLEA, along with one additional agent or other law enforcement official present as a witness, shall review with the CI written instructions that state, at a minimum, that:

(i) the CI is authorized only to engage in the specific conduct set forth in the written authorization described above and not in any other illegal activity;

(ii) the CI's authorization is limited to the time period specified in the written authorization.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

(iii) under no circumstance may the CI:

(A) participate in an act of violence;

(B) participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);

(C) participate in an act designed to obtain information for the JLEA that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search); or

(D) initiate or instigate a plan or strategy to commit a federal, state, or local offense;

(iv) if the CI is asked by any person to participate in any such prohibited conduct, or if he or she learns of plans to engage in such conduct, he or she must immediately report the matter to his or her contact agent; and

(v) participation in any prohibited conduct could subject the CI to full criminal prosecution.

b. Immediately after these instructions have been given, the CI shall be required to sign or initial, and date, a written acknowledgment of the instructions.²⁰ As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the written acknowledgment.

5. Precautionary Measures

Whenever a JLEA has authorized a CI to engage in Tier 1 or 2 Otherwise Illegal Activity, it must take all reasonable steps to: (a) supervise closely the illegal activities of the CI; (b) minimize the adverse effect of the authorized Otherwise Illegal Activity on innocent individuals; and (c) ensure that the CI does not profit from his or her participation in the authorized Otherwise Illegal Activity.

²⁰ The CI may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the CI's files and designated for use by only one CI.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

6. Suspension of Authorization

Whenever a JLEA cannot, for legitimate reasons unrelated to the CI's conduct (e.g., unavailability of the case agent), comply with the precautionary measures described above, it shall immediately: (a) suspend the CI's authorization to engage in Otherwise Illegal Activity until such time as the precautionary measures can be complied with; (b) inform the CI that his or her authorization to engage in any Otherwise Illegal Activity has been suspended until that time; and (c) document these actions in the CI's files.

7. Revocation of Authorization

- a. If a JLEA has reason to believe that a CI has failed to comply with the specific terms of the authorization of Tier 1 or 2 Otherwise Illegal Activity, it shall immediately: (i) revoke the CI's authorization to engage in Otherwise Illegal Activity; (ii) inform the CI that he or she is no longer authorized to engage in any Otherwise Illegal Activity; (iii) comply with the notification requirement of paragraph (IV)(B) below; (iv) make a determination whether the CI should be deactivated pursuant to paragraph (V); and (v) document these actions in the CI's files.
- b. Immediately after the CI has been informed that he or she is no longer authorized to engage in any Otherwise Illegal Activity, the CI shall be required to sign or initial, and date, a written acknowledgment that he or she has been informed of this fact." As soon as practicable thereafter, a Field Manager shall review and, if warranted, approve the written acknowledgment.

8. Renewal and Expansion of Authorization

- a. A JLEA that seeks to re-authorize any CI to engage in Tier 1 or 2 Otherwise Illegal Activity after the expiration of the authorized time period, or after revocation of authorization, must first comply with the procedures set forth above in paragraphs (III)(2)-(5).

The CI may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the CI's files and designated for use by only one CI. If the CI refuses to sign or initial the written acknowledgment, the JLEA agent who informed the CI of the revocation of authorization shall document that the CI has orally acknowledged being so informed and the Field Manager shall, as soon as practicable thereafter, review and, if warranted, approve the written documentation.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- b. A JLEA that seeks to expand in any material way a CI's authorization to engage in Tier 1 or 2 Otherwise Illegal Activity by the JLEA must first comply with the procedures set forth above in paragraphs (III)(C)(2)-(5).

9. Emergency Authorization

- a. In exceptional circumstances, a JLEA's Special Agent in Charge (or the equivalent) and the appropriate Chief Federal Prosecutor may orally authorize a CI to engage in Tier 1 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs (III)(C)(2)-(4) above when they each determine that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 48 hours of the oral approval and maintained in the CI's files.
- b. In exceptional circumstances, a JLEA's Senior Field Manager may orally authorize a CI to engage in Tier 2 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs (III)(C)(2)-(4) above when he or she determines that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 48 hours of the oral approval and maintained in the CI's files.

10. Designees

A JLEA's Special Agent in Charge (or the equivalent) and the appropriate Chief Federal Prosecutor may, with the concurrence of each other, agree to designate particular individuals in their respective offices to carry out the approval functions assigned to them above in paragraphs (III)(C)(2)-(9).

D. LISTING A CONFIDENTIAL INFORMANT IN AN ELECTRONIC SURVEILLANCE APPLICATION

- 1. A JLEA shall not name a CI as a named source or a violator in an affidavit in support of an application made pursuant to 18 U.S.C. § 2516 for an electronic surveillance order unless the JLEA believes that: (a) naming the name of the CI from the affidavit would endanger that person's life or otherwise jeopardize an ongoing investigation; or (b) the CI is a bona fide member of the investigation based on his or her suspected involvement in unauthorized criminal activity.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

2. In the event that a CI is named in an electronic surveillance affidavit under paragraph (III)(D)(1) above, the JLEA must inform the Federal prosecutor making the application and the Court to which the application is made of the actual status of the CI.

IV. SPECIAL NOTIFICATION REQUIREMENTS

A. NOTIFICATION OF INVESTIGATION OR PROSECUTION

1. When a JLEA has reasonable grounds to believe that a current or former CI is being prosecuted by, is the target of an investigation by, or is expected to become a target of an investigation by a FPO for engaging in alleged felonious criminal activity, a Special Agent in Charge (or the equivalent) of the JLEA must immediately notify the Chief Federal Prosecutor of that individual's status as a current or former CI.¹²
2. Whenever such a notification is provided, the Chief Federal Prosecutor and Special Agent in Charge (or the equivalent), with the concurrence of each other, shall notify any other federal, state or local prosecutor's offices or law enforcement agencies that are participating in the investigation or prosecution of the CI.

B. NOTIFICATION OF UNAUTHORIZED ILLEGAL ACTIVITY

1. Whenever a JLEA has reasonable grounds to believe that a CI who is currently authorized to engage in specific Tier 1 or 2 Otherwise Illegal Activity has engaged in unauthorized criminal activity, or whenever a JLEA knows that a CI who has no current authorization to engage in any Tier 1 or 2 Otherwise Illegal Activity has engaged in any criminal activity, a Special Agent in Charge of the JLEA (or the equivalent) shall immediately notify the following Chief Federal Prosecutors of the CI's criminal activity and his or her status as a CI:
 - a. the Chief Federal Prosecutor whose District is located where the criminal activity primarily occurred, unless a state or local prosecuting office in that District has filed charges against the CI for the criminal activity and there clearly is no basis for federal prosecution in that District by the Chief Federal Prosecutor;

¹² A target is "a person as to whom the prosecutor or the grand jury has substantial evidence linking him or her to the commission of a crime and who, in the judgment of the prosecutor, is a putative defendant". U.S.A.M. § 9-11.151.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- b. the Chief Federal Prosecutor, if any, whose District is participating in the conduct of an investigation that is utilizing that active CI, or is working with that active CI in connection with a prosecution; and
 - c. the Chief Federal Prosecutor, if any, who authorized the CI to engage in Tier 1 Otherwise Illegal Activity pursuant to paragraph (III)(C)(2)(a) above.¹³
2. Whenever such notifications are provided, the Chief Federal Prosecutor(s) of the FPOs and the Special Agent in Charge (or the equivalent), with the concurrence of each other, shall notify any state or local prosecutor's office that has jurisdiction over the CI's criminal activity, and that has not already filed charges against the CI for the criminal activity, of the fact that the CI has engaged in such criminal activity. The Chief Federal Prosecutor(s) and the Special Agent in Charge (or the equivalent) are not required, but may with the concurrence of each other, also notify the state and local prosecutor's office of the person's status as a CI.

C. NOTIFICATION REGARDING CERTAIN FEDERAL JUDICIAL PROCEEDINGS.

Whenever a JLEA has reasonable grounds to believe that: (1) a current or former CI has been called to testify by the prosecution in any federal grand jury or judicial proceeding; (2) the statements of a current or former CI have been, or will be, utilized by the prosecution in any federal judicial proceeding; or (3) a federal prosecutor intends to represent to a Court or jury that a current or former CI is or was a co-conspirator or other criminally culpable participant in any criminal activity, a Special Agent in Charge (or the equivalent) of the JLEA shall immediately notify the Chief Federal Prosecutor for that proceeding of the individual's status as a current or former CI.

D. PRIVILEGED OR EXCULPATORY INFORMATION

- 1. In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall notify the attorney assigned to the matter, in advance whenever possible, if the JLEA has reasonable grounds to believe that a CI will obtain or provide information that is subject to, or arguably subject to, a legal privilege of confidentiality belonging to someone other than the CI.

¹³ Whenever such notifications to FPOs are provided, the JLEA must also comply with the Continuing Suitability requirements described above in paragraph (II)(A)(2).

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

2. If the JLEA has reasonable grounds to believe that a current or former CI has information that is exculpatory as to a person who is expected to become a target of an investigation, or as to a target of an investigation, or as to a defendant (including a convicted defendant), the JLEA shall notify the Chief Federal Prosecutor responsible for the investigation or prosecution of such exculpatory information.

E. RESPONDING TO REQUESTS FROM CHIEF FEDERAL PROSECUTORS REGARDING A CONFIDENTIAL INFORMANT

If a Chief Federal Prosecutor seeks information from a Special Agent in Charge (or the equivalent) as to whether a particular individual is a current or former CI, and states the specific basis for his or her request, the Special Agent in Charge (or the equivalent) shall provide such information promptly. If the Special Agent in Charge (or the equivalent) has an objection to providing such information based on specific circumstances of the case, he or she shall explain the objection to the Chief Federal Prosecutor making the request and any remaining disagreement as to whether the information should be provided shall be resolved pursuant to paragraph (I)(G).

F. FILE REVIEWS

Whenever a JLEA discloses any information about a CI to a FPO pursuant to paragraphs (IV)(A)-(E), the Special Agent in Charge (or the equivalent) and the Chief Federal Prosecutor shall consult to facilitate any review and copying of the CI's files by the Chief Federal Prosecutor that might be necessary for the Chief Federal Prosecutor to fulfill his or her office's disclosure obligations.

G. DESIGNEES

A Special Agent in Charge (or the equivalent) and a Chief Federal Prosecutor may, with the concurrence of each other, agree to designate particular individuals in their respective offices to carry out the functions assigned to them in paragraphs (IV)(A)-(F).

V. DEACTIVATION OF CONFIDENTIAL INFORMANTS

A. GENERAL PROVISIONS

A JLEA that determines that a CI should be deactivated for cause or for any other reason, shall immediately:

1. deactivate the individual;
2. document the reasons for the decision to deactivate the individual as a CI in the CI's files;

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

3. if the CI can be located, notify the CI that he or she has been deactivated as a CI and obtain documentation that such notification was provided in the same manner as set forth in paragraph (II)(C)(2); and
4. if the CI was authorized to engage in Tier 1 or Tier 2 Otherwise Illegal Activity pursuant to paragraph (III)(C)(2)(a)-(b), revoke that authorization under the provisions of paragraph (III)(C)(7).

B. DELAYED NOTIFICATION TO A CONFIDENTIAL INFORMANT

A JLEA may delay providing the notification to the CI described above in Paragraph (V)(A)(3) during the time such notification might jeopardize an ongoing investigation or prosecution or might cause the flight from prosecution of any person. Whenever a decision is made to delay providing a notification, that decision, and the reasons supporting it, must be documented in the CI's file.


C. CONTACTS WITH FORMER CONFIDENTIAL INFORMANTS DEACTIVATED FOR CAUSE

Absent exceptional circumstances that are approved by a Senior Field Manager, in advance whenever possible, an agent of a JLEA shall not initiate contacts with, or respond to contacts from, a former CI who has been deactivated for cause. When granted, such approval shall be documented in the CI's file.

D. COORDINATION WITH PROSECUTORS

In situations where a FPO is either participating in the conduct of an investigation by a JLEA that is utilizing a CI, or working with a CI in connection with a prosecution, the JLEA shall coordinate with the attorney assigned to the matter, in advance whenever possible, regarding any of the decisions described in paragraphs (V)(A)-(C).

Date: May 30, 2002


John Ashcroft
Attorney General

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

APPENDIX IX

DEA RESPONSE TO THE DRAFT AUDIT REPORT



U. S. Department of Justice
Drug Enforcement Administration

DEA-SENSITIVE

www.dea.gov

Washington, D.C. 20537

MAR 15 2005

MEMORANDUM

TO: Guy K. Zimmerman
Assistant Inspector General for Audit

FROM: *Michelle M. Donohue*
Michelle M. Donohue
Deputy Administrator

SUBJECT: Draft Audit Report: *The Drug Enforcement Administration's Payments to Confidential Sources*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ), Office of the Inspector General's (OIG) draft audit report entitled *The Drug Enforcement Administration's Payments to Confidential Sources*. DEA provides the following comments as requested in your memorandum dated February 22, 2005.

Based upon the review of the report, DEA concurs with recommendations 1a, 5, 6, 7, 8, and 9 resulting from this audit and will take steps to implement the recommendations. DEA believes recommendations 1b, 2, and 10 are related to compliance with existing policy, requiring a reinforcement of the policy as opposed to establishment of new policy. In fact, OIG notes that DEA exceeds DOJ standards for continuing suitability reports of confidential sources. Similarly, recommendations 1c, 1d, 3, 4, 11, and 12 are directed at areas of DEA's confidential source program where policy and procedure exists to address these concerns. Based on clarifying information provided in the comments below and the attached Action Plan, DEA requests OIG to close recommendations 1d, 3, 4, 11, and 12. Corrective measures articulated in the Action Plan will be implemented to close the remaining recommendations.

The audit of DEA's payments to confidential sources was initiated in July 2002, less than one year following the terrorist attacks in New York City, Pennsylvania, and Washington, D.C. on September 11, 2001. During the aggressive federal law enforcement investigation following the attacks, the depth and value of DEA's human intelligence program was acknowledged by both the federal law enforcement community and the Intelligence Community. DEA's confidential sources, operating in domestic and foreign environments at the direction of the agency's dedicated and virtuous criminal investigators, are the core of this program. The identification and investigation of links between drug trafficking organizations and terrorist groups is dependent on the invaluable

DEA-SENSITIVE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Guy K. Zimmerman, Assistant Inspector General for Audit

Page 2

information and contributions of DEA-controlled confidential sources. In many cases, the evidence gleaned by confidential sources is key to the successful prosecution and dismantlement of entire drug trafficking organizations.

As the report accurately reflects, confidential sources cooperate with DEA for a variety of reasons, to include financial gain and altruism. In all instances, to include confidential sources operating in the most precarious and dangerous environments, DEA strives to protect the identity of its confidential sources. Perhaps more than financial gain, confidentiality is the crux of recruitment and utilization of confidential sources in the pursuit of justice against the world's most dangerous drug trafficking organizations. Policy related to the management of DEA's confidential sources reflects procedures to effectively and safely control confidential sources and comply with established departmental guidelines.

Like all audits, the process of successfully soliciting, reviewing, and evaluating information deemed necessary for the review is contingent upon OIG and DEA having a mutual understanding of the scope and specification of information required to conduct the review. Information contained in the report pertaining to confidential source payment information from DEA's Federal Financial System (FFS) indicates that DEA personnel could have improved the communication of existing DEA policy and information to OIG auditors. DEA has elevated its audit liaison function within the agency to the Executive Policy and Strategic Planning Staff to more effectively facilitate this process between its program offices of record and OIG auditors.

FFS is the accounting system used by DEA, for which it and the agency's financial controls have received an unqualified opinion from independent auditing firms. DEA disagrees with the report's implications that FFS is unreliable and its characterization as a system that "handles the DEA financial information." It is a comprehensive financial management system designed specifically for federal agencies; FFS provides financial accounting, fund control, and financial reporting processes. All transactions using DEA funding from appropriations, fees, reimbursable and transfer authorities are recorded in the general ledger in FFS. As has been demonstrated by six consecutive years of unqualified audit opinions, from fiscal years 1999 through 2004, the FFS accounting system provides accurate, reliable, and valid financial and accounting records to support DEA operations. Indeed, in Appendix I, on page 56, the OIG states:

"We did not perform testing to express an opinion on the Federal Financial System, and therefore we do not express an opinion on it. However, as a part of the annual financial statement audit, the DEA financial management systems are reviewed to determine their compliance with the federal financial management systems requirements, applicable federal accounting standards, and the United States General Ledger. These systems were found to comply with these requirements for the [fiscal year] FY 2003 financial statement audit. Therefore, we believe that the data used for our sampling and testing purposes was reliable to the extent needed."

On pages 26 through 29, confidential source payment information for fiscal years 1998 through 2001 is presented and discussed. The report indicates that the same information was requested in July 2002 and June 2003, and significantly different responses were provided each time. The report

DEA-SENSITIVE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- 108 -

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Guy K. Zimmerman, Assistant Inspector General for Audit

Page 3

incorrectly implies that FPS is unreliable and produces different results each time it is queried. The information provided in July 2002 was from DEA's Confidential Source System (CSS), not FPS, and was based on fiscal year. The information provided in June 2003 was from FPS and based on budget fiscal year from 1998 through 2001. Thus, the information provided is not comparable.

DEA's current confidential source policy was found to be compliant with the Attorney General's Guidelines Regarding the Use of Confidential Informants by DOJ in January 2004. DEA's policy addresses initial suitability reports, written continuing suitability reports, long-term confidential source assessment reviews, confidential source categorization, and DEA Form 103 utilization. DEA acknowledges the exceptions to policy compliance identified by OIG auditors during its review, but the policy is deemed to meet the standards established by DOJ. Notwithstanding, DEA agrees to take action to strengthen its confidential source policy by requiring and maintaining documented initial suitability reports. Additionally, DEA will reaffirm management's role in ensuring policy compliance in response to recommendations 1b, 2, and 10 as noted on the Action Plan. Compliance with existing policy will alleviate the concerns noted by OIG in these areas.

DEA's policy regarding the category of Limited Use confidential sources is a part of DEA's confidential source policy, which was approved by DOJ in January 2004. The policy related to Limited Use confidential sources is exhaustively delineated under Section 6612.22 of the *Agency Manual*. Essentially, this category of informant is a Source of Information (an individual, acting independently or as a representative of a group or organization, who provides information or services to DEA that does not meet established criteria for a confidential source) that is a "professional" business person or is a "tipster" who is established as a Limited Use confidential source for payment purposes only.

In order to receive payment, a criminal history check is required in addition to other law enforcement indices checks. The policy is clear that a Limited Use confidential source will not testify, be named, or have any criminal association. Limited Use establishments does not grant the confidential source from adhering to the Attorney General's Confidential Informant Guidelines for monetary purposes. The Limited Use status allows for a waiver of the Initial Suitability Report and Recommendation, the Initial Denial, and the acquisition of fingerprints and photographs of the prospective confidential source. This exemption was approved by DOJ with the understanding that these sources are not involved in any criminal matter and will not be required to testify as a witness in any legal proceedings.

DEA-SENSITIVE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Gary K. Zimmerman, Assistant Inspector General for Audit

Page 4

DEA's Office of Inspections (OI) includes a review of both confidential source and underlying investigative files in its on-site inspections. It is important to note that the value of confidential source information can only be fully assessed through reviews of both the confidential source and underlying investigative files. These file reviews are used by OI to assess the enforcement effectiveness of the office and assess whether or not confidential sources are being properly utilized. These complete reviews are the basis for determining the value of information gleaned in contrast to the payments made to confidential sources and identifying any indications of integrity-related violations. In regard to OIG's assessment of signature exemplars and the related recommendation, DEA believes the confidential source's initial signature on the DEA Form 473 "Confidential Source Agreement," and its annual re-execution, sufficiently provides an exemplar for comparison purposes during on-site inspections and any integrity-related investigations.

OIG auditors reviewed the forms and approval levels of DEA's confidential source payment system as part of the audit. DEA notes several areas of the report that do not fully articulate existing policy and procedures in these areas. OIG notes on page 52 of the report that a required SES-level approval was not found on the DEA Form 103, when in actuality, instances that confidential source payments are made from the Asset Forfeiture Fund, SES-level approval is noted on a DEA Form 499, "Request for Payment from the Asset Forfeiture Fund." Additionally, OIG notes that DEA Form 12a and receipts were consistently found not to be attached to DEA Form 103a to support payments. DEA Form 12a are considered fiscal documents and are contained in administrative files as part of the financial record. It is DEA's policy to obtain receipts for expenses incurred by confidential sources whenever possible and attach the same to the file copy of the DEA Form 103. A requirement to obtain receipts is not considered practical and most importantly, presents numerous safety issues for confidential sources operating at the direction of DEA Special Agents.

DEA agrees with needed improvements to the CSS (Confidential Source System) and has already begun action to update the system; however, the system currently possesses the capability and is already used to electronically capture relevant confidential source impeachment information. Improvements to be implemented include the capability to track payments from both appropriated and non-DEA funds, the ability to only update the CSS through the FPS interface for confidential sources in an active status, and the ability to more accurately track calendar year and lifetime payment caps. While improvements to the CSS will allow for the inclusion of non-DEA funds, these funds are not included in DEA's financial statements and are not and should not be maintained in DEA's general ledger or FPS. A formal, documented reconciliation process will be implemented along with the new system to ensure that all payments made to DEA confidential sources are reconciled on a regular basis.

DEA has completed a sensitivity review of the draft audit report. This information is provided under separate cover.

Documentation detailing DEA's efforts to implement the attached action plan will be provided to OIG until all corrective actions are completed. If you have any questions regarding this information, please contact Audit Liaison Shelley Sheen at (202) 307-4205.

Attachments

DEA-SENSITIVE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- 110 -

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Guy K. Zimmerman, Assistant Inspector General for Audit

Page 5

CC: Richard P. Thole
Acting Director, Audit Liaison Office
Justice Management Division

DEA-SENSITIVE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- 111 -

ACTION PLAN**The Drug Enforcement Administration's Payments to Confidential Sources**

Recommendations	Action Planned	Proposed Completion Date
<p>1. Update the "DEA Agent Manual" to:</p> <p>a. Require comprehensive written Initial Suitability Reports that address all of the factors specified in the "Attorney General Guidelines."</p>	<p>As approved by the Department of Justice (DOJ) in January 2004, DEA's confidential source policy uses the terminology of Risk Assessment and Suitability Statement for what the Attorney General's Guidelines Regarding the Use of Confidential Informants (AGG) terms Initial Suitability Report and Recommendations (ISRR). All the factors required by the DOJ ISRR regarding the assessment of prospective confidential source are also required by the DEA to be addressed and documented during confidential source establishment (See 6612.32, A&B of the "Agents Manual"). Although the current DEA confidential source policy is in full compliance with the standards set forth within the AGG, the Office of Operations Management (OM) will amend the existing confidential source policy to require the Initial Risk Assessment now be documented and maintained in the confidential source file. The DEA Form 371 will continue to be used to verify the Risk Assessment and Suitability review have been completed (Block 30), and to document in paragraph four any known disqualifying issues identified as a result of this assessment (Block 39). OM will issue a teletype to field offices reflecting an interim amendment to the DEA confidential source policy to require the above change, until such time a permanent change to the policy is made.</p>	June 30, 2005
<p>1. Update the "DEA Agent Manual" to:</p> <p>b. Require written continuing suitability reports that address all the factors specified in the "Attorney General Guidelines."</p>	<p>The AGG requires that the Continuing Suitability Review be completed on an annual basis. DEA's confidential source policy exceeds the DOJ mandate by requiring the review four times a year as the Quarterly Management Review of Confidential Source Utilization (QMRCU). Section 6612.6</p>	June 30, 2005

DEA-SENSITIVE

ACTION PLAN

The Drug Enforcement Administration's Payments to Confidential Sources

Recommendations	Action Planned	Projected Completion Date
	<p>of the "Agents Manual" clearly stipulates that the ISRR factors be addressed and documented.</p> <p>OM will issue a teletype to all field managers that reinforces the requirements set forth in Section 6612.6 of the "Agents Manual."</p>	
<p>1. Update the "DEA Agent Manual" to:</p> <p>c. Require the Sensitive Activity Review Committee to either review the confidential source files for all long-term confidential sources, or review the continuing written Initial and Suitability Reports and Recommendations, and document their findings.</p>	<p>The AOG requires that a Confidential Informant Review Committee be convened to review long-term informants every six years. Long-term is defined as being in a continuing active status of six years or more. The DOJ-approved DEA confidential source policy exceeds the AOG by reviewing annually every long-term informant. This review is conducted by the DEA Sensitive Activity Review Committee and has occurred twice since the current policy's implementation. The methodology used is that OM queries the Confidential Source System (CSS) database to identify all relevant informants and notifies the respective field offices by teletype of the pending review. Each Special Agent in Charge (SAC) must then review the complete, local confidential source file, and prepare and submit his/her synopsis and recommendation regarding future use of the confidential source to OM in memorandum form. In addition, the SARC is provided a comprehensive spreadsheet summary of information gleaned as a result of the SAC's review. In accordance with Section 6612.43(F) of the "Agents Manual," copies of confidential source files, containing all QMRCsUs, stored at DEA Headquarters are made available for SARC review as well. It should be noted that all SARC reviews require the participation and</p>	<p>Pending OIG Review</p>

DEA-SENSITIVE

ACTION PLAN

The Drug Enforcement Administration's Payments to Confidential Sources

Recommendations	Action Planned	Projected Completion Date
<p>1. Update the "DEA Agent Manual" to:</p> <p>d. Clarify the process for establishing Limited Use confidential sources to include demonstrating how the DEA can be assured the individual is eligible for Limited Use status and how this status either complies with or is exempt from the "Attorney General Guidelines."</p>	<p>consequence of DOJ's sensitive and Dangerous Drug Section. DEA will make copies of these documents available for review by OIG to clear the recommendation.</p> <p>DEA's policy regarding the category of Limited Use confidential sources is a part of DEA's confidential source policy, which was approved by DOJ in January 2004. The policy related to Limited Use confidential sources is extensively delineated under Section 6512.22 of the "Agent Manual." Essentially, this category of informant is a Source of Information (an individual, acting independently or as a representative of a group or organization, who provides information or services to DEA that does not meet established criteria for a confidential source) that is a "professional" businessperson or is a "speaker" who is established as a Limited Use confidential source for payment purposes only.</p> <p>In order to receive payment a criminal history check is required in addition to what law enforcement indices checks. The policy is clear that a Limited Use confidential source will not testify, be directed, or have any criminal disposition. Limited Use establishment does not exempt the confidential source from adhering to the AOC's requirements for monetary payments. The Limited Use status allows for a waiver of the Initial Suitability Report and Recommendation, the Initial Debriefing, and the acquisition of fingerprints and photographs of the prospective confidential source. This exemption was approved by DOJ with the understanding that these sources are not involved in any criminal matter and</p>	<p>Pending Closure Request</p>

DEA-SENSITIVE

ACTION PLAN

The Drug Enforcement Administration's Payments to Confidential Sources

Recommendations	Action Planned	Projected Completion Date
	will not be required to testify as a witness in any legal proceeding. Based on this clarification, DEA requests OIG close this recommendation.	
2. Implement a policy of documenting the rationale for confidential source's categorization.	Based on the results of the Risk Assessment and other factors gathered during the preparation for confidential source establishment, the category type is determined by field agents based upon the specific criteria outlined under Section 6612.2 of the "Agent Manual." The category of confidential source is documented on block 27 of the DEA Form 312, and the situation qualifying the Source type is documented on block 29, "Source Type Qualification" of the DEA Form 312. DEA will issue a teletype to all field managers that reiterates Section 6612.2 of the "Agent Manual."	June 10, 2005
3. Consider adding a module to the Confidential Source System that tracks confidential source impeachment information.	Impeachment information regarding active confidential sources is documented on OIRCSUs or, if severe enough, an indictment, within the Management Review process (Section 6612.74(B) of the "Agent Manual"). If the confidential source is deactivated either for cause or to the level of being declared "Unsatisfactory," the information will be documented on the deactivation report (DEA Form 6). In all these cases, the circumstances are noted in the Remarks portion of the CSS record so that Confidential Source Coordinators DEA-wide can readily be made aware of the existence of impeachment information. The CSS is required to be queried prior to any establishment.	Pending Closure Request

DEA-SENSITIVE

ACTION PLAN

The Drug Enforcement Administration's Payments to Confidential Sources

Recommendations	Action Plan	Proposed Completion Date
4. Specifically identify what types of payments are to confidential sources and consistently identify those payments in the Federal Financial System. The DEA should pay specific attention to Budget Object Code 2533 - Payments to Foreign Police Officials and resolve an inconsistency between the Confidential Source Unit and the Office of Finance as to whether payments using Budget Object Code 2533 are confidential source payments.	<p>Based on this clarification, DEA requests OIG file this recommendation.</p> <p>[REDACTED]</p> <p>The following payment categories are for CSS and imported nightly from the FPS into the respective CSS records:</p> <ol style="list-style-type: none"> 1. Payment for information (BOC 2530) 2. Reward payments (2534) 3. Witness security or relocation (2536) 4. Asset Forfeiture Fund (2599, 2579) <p>[REDACTED]</p> <p>Based on this clarification, DEA requests OIG file this recommendation.</p>	<p>Pending Closure Request</p> <p>15(7)(E)</p>
5. Document the payment process for payments using non-appropriated funds (specifically High Intensity Drug Trafficking Areas) and develop an automated method to track those payments.	DEA will implement this recommendation in conjunction with the new CSS currently under construction. The module incorporating payment information is scheduled for implementation in Phase 2 of the system construction process. Phase 1 of the process should go into production in October 2005. Assuming a smooth transition into Phase 1 of the new system, the planning, budgeting, and construction of Phase 2 should be accomplished by October 2006.	October 1, 2006

DEA-SENSITIVE

ACTION PLAN**The Drug Enforcement Administration's Payments to Confidential Sources**

Recommendations	Action Planned	Projected Completion Date
6. Account for all payments made to a confidential source by the DEA, not just payments using DEA-appropriated funds.	All payments made by DEA to a DEA confidential source using appropriated and non-appropriated funds are required to be documented on the DEA Form 356, which is maintained in the responsible field office confidential source file. The new CSS will completely automate this requirement by October 2006, as stated above.	October 1, 2006
7. Implement a formal process to reconcile all payments to confidential sources, both from appropriated and non-appropriated funds, to the Federal Financial System, the CSS Dollar database, and any other medium used to account for non-appropriated fund payments, such as HIDA interest funds. This process should clearly identify who is responsible for the reconciliation, the time period the reconciliation should cover, and who approves the completed reconciliation.	The new CSS will include confidential source payments made by DEA from both appropriated and non-appropriated funds. The payment module is expected to be implemented by October 2006. A formal, documented reconciliation process will be implemented along with the new system to ensure that all payments to confidential sources are reconciled on a regular basis.	October 1, 2006
8. Enhance controls over confidential source payments to prevent a deactivated confidential source or administratively closed case from being used to obligate or expend funds.	Under the current CSS, a temporary project is under way to revamp the nightly data feed of information to the FFS to provide only the confidential source numbers of those in an active status. The new CSS will have this designed as an inherent capability. DEA will request closure of this recommendation upon certification by OM that the nightly data feed only contains confidential sources in an active status.	June 30, 2005

DEA-SENSITIVE

ACTION PLAN**The Drug Enforcement Administration's Payments to Confidential Sources**

Recommendations	Action Planned	Projected Completion Date
9. Develop a plan to correct the CSS Dollar database to reflect accurate, up-to-date data on confidential source payments and implement an audit trail to identify what changes were made to the electronic records. Alternatively, the DEA should develop another electronic process for monitoring calendar year and lifetime payments to confidential sources. If the DEA develops another electronic process, the "DEA Agent Manual" should be amended to reflect this new process.	Currently, received CSSS information is accurate for DEA appropriated funds. The new CSS will have the added ability to electronically track non-appropriated payments. Policy will be amended as necessary to explain how the new CSSS information monitors calendar year and lifetime payments.	October 1, 2006
10. Reinforce guidance to agents on the requirements of completing a voucher for Purchase of Evidence or Payment to Confidential Source (DEA 103). The reinforcement should address all sections of a complete DEA 103 including purpose of payment, remarks, signature, and fund citation, as well as obtaining receipts when possible or document why a receipt is not possible.	OM will issue a teletype to all field offices that reinforces the instructions for completing the DEA Form 103 and to ensure that the fund cite appears on the confidential source file copy.	June 30, 2005
11. Amend the "DEA Agent Manual" to require that Receipts for Cash or Other Items (DEA 12) be attached to DEA 103 if the DEA 12 is used to document the appropriate manager level approval.	DEA Form 12s are considered legal documents and are contained in administrative files as part of the financial record. Additionally, it is DEA's policy to obtain receipts for expenses incurred by confidential sources whenever possible and attach the same to the file copy of the DEA Form 103. A requirement to obtain receipts is not considered practical and most importantly, presents numerous safety issues for confidential sources operating at the direction of DEA Special Agents. Based on this clarification, DEA requests OIG close this recommendation.	Pending Closure Request

DEA-SENSITIVE

ACTION PLAN

The Drug Enforcement Administration's Payments to Confidential Sources

Recommendations	Action Planned	Project Completion Date
12. Consider reinstating a requirement to obtain signature exemplars for confidential sources.	<p>During the preliminary confidential source establishment and evaluation phase, a clear signature is provided by the confidential source when signing the DEA Form 473, Confidential Source Agreement. This process is conducted during all confidential source establishment and re-establishments, and like all confidential source-related contact, is mandated by DEA's policy to be conducted by at least two officials. Additionally, the form is re-executed annually for those confidential sources remaining in active status, at which time another signature is obtained from the confidential source.</p> <p>DEA has considered OIG's recommendation and believes the existing practice sufficiently addresses any concerns. DEA requests OIG close this recommendation.</p>	Pending Closure Request

DEA-SENSITIVE

APPENDIX X

**OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND
SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT**

We provided a draft audit report to the DEA for review and comment. The response from the DEA is incorporated as Appendix IX of this final report. In its response to the report, the DEA provided general comments regarding Limited Use Confidential Sources and our finding on the effectiveness for tracking confidential source payments. Our analysis of the DEA's general comments is provided in the first part of this appendix. The second part of this appendix contains our analysis of DEA's response to the 12 recommendations.

DEA's General Comments

Limited Use Confidential Sources

In its response, the DEA stated that its policy regarding the category of Limited Use confidential sources is part of DEA's confidential source policy that was approved by the DOJ in January 2004. The DEA is correct in stating that the Limited Use establishment does not exempt the confidential source from adhering to the Attorney General Guidelines' requirements for monetary payments. However, we do not agree that approval by the DOJ of this confidential source category constitutes an exemption (as defined by the Attorney General Guidelines) from the documentation requirements specified in the Attorney General Guidelines as indicated in DEA's response.

Confidential Source Payments

In its response, the DEA stated that our finding on the confidential source payment system incorrectly implies that the Federal Financial System (FFS) is unreliable and produces different results each time it is queried. The DEA stated that the information provided in July 2002 was from DEA's CSS, not FFS, and was based on fiscal year. The information provided in June 2003 was from FFS and based on budget fiscal year from 1998 through 2001; therefore, the information provided was not comparable.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

Several factors led our determination that the DEA does not have an effective or accurate confidential source payment system. One of those factors is that we received differing confidential source payment amounts from the DEA. We repeatedly requested the DEA to provide explanations for the different payment amounts, and were told after numerous requests that all the data we were previously provided came from the FFS.

As part of our review to assess how the DEA accumulates confidential source payment information, the DEA provided us with the total amount of confidential source payments from FY 1998 through FY 2002 by budget category, which we received in July 2002. One of the budget categories identified in this listing was BOC [REDACTED] even though it did not identify any dollars. (b)(7)(C)

In April 2003, the DEA provided us detailed transactions regarding FY 2001 confidential source payments, which was \$11 million less than the total amount supplied in July 2002. We followed up with the DEA on this discrepancy, which led to DEA providing us payment information in June 2003 that contained dollars associated with BOC [REDACTED] and eventually the quote cited in our report from the previous audit liaison. Therefore, it was DEA's response that led us to believe the FFS produced different results every time it was queried. The DEA now contends that the information provided in July 2002 was from the CSS Dollar system and not the FFS. However, this was not presented to us during the audit. Nevertheless, several DEA confidential source coordinators stated that the CSS Dollar was unreliable.

We also discussed the conflicting information with both the DEA finance office and the Unit Chief of the confidential source unit. The DEA finance office stated that BOC [REDACTED] was not a confidential source BOC; however, the Unit chief stated it was and did not have an explanation for the different treatment the DEA finance office had for BOC [REDACTED]. This conflict also added to our determination that the DEA does not have an effective or accurate system for tracking confidential source payments.

The DEA acknowledged however that its personnel could have improved the communication of existing DEA policy and information to the OIG auditors. To better facilitate the communication between its program offices and OIG auditors, the DEA has since elevated its audit liaison function within the agency to the Executive Policy and Strategic Planning Staff.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

As part of our audit, we reviewed the process agents use to pay confidential sources including the forms and the approval levels needed. The DEA response stated that the OIG did not fully articulate the existing policy and procedures with regard to approval levels and the maintenance of certain documentation:

- On page 52 of the report, we noted an Asset Forfeiture Award for \$1.25 million that contained the required Headquarters approval, but we were unable to verify the required division SES-level approval on the "Voucher for Purchase of Evidence or Payment to Confidential Source" (DEA 103). The DEA stated that a Senior Executive Service (SES) level signature on the DEA 499, "Request for Payment from the Asset Forfeiture Fund," is sufficient and need not be on the DEA 103. However, the DEA 499 is only a request for asset forfeiture award money and not the actual payment. We could not find anywhere in the DEA Agent Manual where it states an SES-level signature on the DEA form 499 is all that is needed when this type of payment is made. Rather, the DEA Agent Manual, section 6612.57, states all asset forfeiture awards will be documented on a DEA 103 and further states in section 6612.52 D that payments over \$25,000 need SES approval.
- During our audit, we could not verify that appropriate approvals were received for payments exceeding \$2,500 because in many instances the DEA 103 did not reflect the appropriate supervisory approval. According to the Unit Chief of the Confidential Source Unit, a "Receipt for Cash or Other Items" (DEA 12) should be attached to the DEA 103 if the required supervisor approval of the payment is on the DEA 12 and not on the DEA 103. In its response, the DEA stated that DEA 12s are considered fiscal documents and are contained in administrative files as part of the financial record, not the confidential source file. Our report notes that the DEA does not require the DEA 12 to be filed in the confidential source file. However, the impetus for our finding and recommendation was the fact that in 66 of 439 instances, the DEA 103 did not reflect the appropriate supervisory approval, and DEA could not locate the DEA 12 in the administrative files.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

In the DEA action plan, the DEA indicates a new CSS will be developed and implemented that will account for all the payments to confidential sources regardless if the payments are from appropriated or non-appropriated funds. The DEA specifies that the non-appropriated fund payments will not be included in the financial statements, the general ledger, or FFS. The OIG agrees that the non-appropriated payment information should not be in the DEA financial statements, general ledger or FFS as evidenced by recommendation number 7 which talks about "any other medium used to account for non-appropriated fund payments."

Response to Recommendations

- 1a. **Resolved.** This recommendation is resolved based on the DEA's action to amend existing confidential source policy to require the initial risk assessment to be documented and maintained in the confidential source file. This recommendation can be closed when we receive and review the amended policy.
- b. **Resolved.** This recommendation is resolved based on the DEA's plan to issue a teletype to all field managers that reinforces the requirements set forth in Section 6612.6 of the "Agents Manual." However, we believe the DEA policy needs to be revised to require the documentation of each factor specified in the Attorney General Guidelines. This recommendation can be closed when we receive and review the direction to field managers requiring all factors specified in the Attorney General Guidelines be addressed and documented in the continuing suitability review.
- c. **Resolved.** According to the Attorney General Guidelines, when a confidential source has been registered for more than six consecutive years, and to the extent such a source remains open every six years thereafter, the SARC shall review the completed Initial and Continuing Suitability Reports and Recommendations. Therefore, this recommendation can be closed when the DEA provides us with the sample documents that will be made available for the SARC's review, and requires the written initial suitability review be provided to the SARC in addition to the Quarterly Management Review of Confidential Source Utilization.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

- d. **Resolved.** In its response, the DEA stated that its policy regarding the category of Limited Use confidential sources is a part of DEA's confidential source policy that was approved by the DOJ in January 2004. The DEA is correct in stating that the Limited Use establishment does not exempt the confidential source from adhering to the Attorney General Guidelines' requirements for monetary payments. However, we do not agree that approval by the DOJ of this confidential source category constitutes a blanket exemption from the documentation requirements specified in the Attorney General Guidelines as indicated in DEA's response.

The Attorney General Guidelines state that when an entity to which these Guidelines apply believes that an exception to any provision of the Guidelines is justified; an exception must be sought from the Assistant Attorney General (AAG) for the Criminal Division or his or her designee. Any exception granted shall be documented in the entity's files. Therefore, in order to close this recommendation, the DEA should provide the exemption received for the Limited Use confidential source. Otherwise, it should revise its policy to require the Attorney General Guidelines' minimum documentation requirements for paid sources

2. **Resolved.** This recommendation is resolved based on the DEA's planned action to reinforce the requirement to document the rationale for the confidential source's categorization on the DEA 512. This recommendation can be closed when we receive and review the directive to all field managers and ensure that the directive adequately specifies the documentation needed to support the rationale for a specific categorization.
3. **Resolved.** The DEA's response states that processes are in place to capture and track Impeachment Information and no further action is necessary. However, at a minimum, the DEA should consider issuing a teletype to all Confidential Source Coordinators notifying that *all* impeachment information must be included in the Remarks portion of the CSS record. This recommendation can be closed when the DEA provides us with such notice or reasons why such a notice should not be issued.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

4. **Resolved.** This recommendation is resolved because the DEA response clearly identifies what payments are confidential source payments and specifically identified those payments. However, we believe this clarification should be incorporated into the DEA Agent Manual. This recommendation can be closed when the DEA incorporates this clarification in the *Agent Manual*.
5. **Resolved.** This recommendation is resolved based on the DEA's action to develop a new CSS that will provide an automated method to track non-appropriated funds (specifically High Intensity Drug Trafficking Areas) payments. This recommendation can be closed when we receive and review documentation of the payment process for payments using non-appropriated funds (specifically High Intensity Drug Trafficking Areas) and when the DEA has fully implemented an automated system for tracking payments using non-appropriated funds.
6. **Resolved.** This recommendation is resolved based on the DEA's action to develop a new CSS that will provide an automated accounting of all payments made to confidential sources. This recommendation can be closed when the DEA has fully implemented the new CSS that tracks all payments made to confidential sources.
7. **Resolved.** This recommendation is resolved based on the DEA's action to develop a new CSS that will provide an automated method to track all confidential source payments. This recommendation can be closed when we receive and review documentation of the reconciliation process including who is responsible, the time period and the approval authority, and when the DEA fully implements the new CSS that tracks all payments made to confidential sources.
8. **Resolved.** This recommendation is resolved based on the DEA's action to develop a new nightly feed of information from CSS that will prevent deactivated confidential source numbers from being used to obligate or expend funds. This recommendation can be closed when the DEA has fully implemented the new CSS that will prevent deactivated confidential source numbers from being used to obligate or expend funds and when the DEA enhances controls to prevent administratively closed cases from being used to obligate or expend funds.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

9. **Resolved.** This recommendation is resolved based on the DEA's planned corrective action to develop a new CSS that will accurately track all confidential source payments. This recommendation can be closed when the DEA meets the requirements to close recommendation 5, 6, 7, and 8, and amends the DEA Agent Manual to reflect the revised process for monitoring calendar and lifetime payments

The DEA states in its response that the current CSS Dollar information is accurate for DEA Appropriated funds. This contradicts 5 of 7 Confidential Source Coordinators we interviewed and numerous e-mails that specify the information in CSS Dollar is unreliable. Given that the DEA does not currently have a formal reconciliation process, we do not have basis to agree with the DEA's contention that CSS Dollar is accurate.

10. **Resolved.** This recommendation is resolved based on the DEA's planned action to reinforce instructions on completing a DEA 103 including ensuring the fund cite appears on the confidential source file copy. This recommendation can be closed when we receive and review the DEA teletype to all field offices that provides instructions for completing a DEA 103, including instructions on documenting the fund citations on the confidential source copy of the DEA 103 and instructing agents that receipts are to be obtained whenever possible or the agent must document why a receipt is not possible.
11. **Unresolved.** This recommendation is unresolved because the DEA's response does not address the recommendation. Regardless of whether the DEA 12 is a fiscal document, if the DEA 12 is the only document that supports the appropriate approval of a payment, it should be included in the confidential source file with the corresponding DEA 103. Otherwise a reviewer could not determine if the payment was appropriately authorized without going to another file. During our audit, when we requested the DEA 12 to validate the appropriate approval, DEA could not always locate the requested DEA 12.
12. **Closed.** This recommendation is closed. Because the DEA appears to have carefully considered our recommendation, we are closing this recommendation. However, we continue to recommend that the DEA consider using signature exemplars.

LIMITED OFFICIAL USE - NOT FOR PUBLIC RELEASE

