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

Audit of the Drug Enforcement Administration's Management and Oversight of its Confidential Source Program

Audit Division 16-33 September 2016

AUDIT OF THE DRUG ENFORCEMENT ADMINISTRATION'S MANAGEMENT AND OVERSIGHT OF ITS CONFIDENTIAL SOURCE PROGRAM

EXECUTIVE SUMMARY

The Drug Enforcement Administration (DEA) considers its Confidential Source Program to be critical to its pursuit of illegal narcotics trafficking. However, confidential sources can be motivated by factors other than combating crime, including financial gain and avoidance of punishment; therefore, care must be taken to evaluate and supervise their use. Between October 1, 2010, and September 30, 2015, the DEA had over 18,000 active confidential sources assigned to its domestic offices, with over 9,000 of those sources receiving approximately $237 million in payments for information or services they provided to the DEA.

In July 2015, the Department of Justice (Department or DOJ) Office of the Inspector General (OIG) issued a report on the DEA's confidential source policies and its oversight of higher-risk confidential sources. We found the DEA's confidential source policies were not in full compliance with the Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines).

In this review, we concluded that DEA's management and oversight of, and policies governing, its Confidential Source Program required significant improvement. In particular, we found DEA field offices bear disproportionate responsibility for confidential source management and review. For example, DEA headquarters offices do not provide comprehensive oversight to ensure that field offices' establishment and use of sources, and payments to them, are appropriate, reasonable, and justified.

We found that the DEA did not adequately oversee payments to its sources, which exposes the DEA to an unacceptably increased potential for fraud, waste, and abuse, particularly given the frequency with which DEA offices utilize and pay confidential sources. For example, while DEA policy prohibits paying deactivated sources who were deactivated because of an arrest warrant or for committing a serious offense, we found two concerning instances of payments to previously-deactivated sources. In one case, the DEA reactivated a confidential source who previously provided false testimony in trials and depositions. During the approximate 5-year period of reactivation, this source was used by 13 DEA field offices and paid $469,158. More than $61,000 of the $469,158 was paid after this source was once again deactivated for making false statements to a prosecutor.

This was not the only confidential source who received payments after having been deactivated. Based on our review of DEA's confidential source data, we estimated the DEA may have paid about $9.4 million to more than 800 deactivated sources between fiscal years (FY) 2011 and 2015. While we describe in this report some concerns about the accuracy and completeness of the available DEA data, and while we did not review the circumstances of all of these payments in depth, from

available information it appears that paying deactivated sources is common enough to justify much closer managerial oversight and review of such payments.

Another area of concern is the DEA's oversight of confidential sources it categorized as "Limited Use," often referred to as "tipsters," which DEA policy specifies are sources who make information available independently without direction by the DEA. The Limited Use category is regarded by the DEA as low-risk and therefore DEA policy requires the least supervision. Yet we found that Limited Use sources were some of DEA's highest paid sources, with 477 Limited Use sources during the period of our review having received an estimated $26.8 million.

We reviewed confidential source files associated with six DEA field offices with interdiction units – enforcement units whose primary activity is to intercept drug trafficking at transportation and other facilities. We found these units relied heavily on Limited Use confidential sources who were employees in the travel and parcel industries with access to passenger information or private facilities. We also found that Special Agents gave instructions and guidance to these sources about what information to provide the interdiction units and what actions to take to assist them, testing the boundaries of what it means to provide information "without direction." For example, some Agents requested that sources provide them with suspicious travel itineraries that met criteria defined by the Agents, and in some cases requested entire passenger manifests almost daily. Similarly, some parcel employees were told to provide information related to suspicious parcels and, at times, followed DEA instructions to directly transfer customer packages to the DEA. Some of these sources received significant payments for their assistance, including an airline employee who received more than $600,000 in less than 4 years, and a parcel employee who received over $1 million in 5 years. We believe that DEA Agents directed the actions of these sources extensively enough that they could not reasonably be understood to have acted "without direction" and therefore do not fit the definition or purpose of "Limited Use."

Among the Limited Use sources the DEA established were Amtrak and Transportation Security Administration (TSA) employees. In November 2015, the OIG completed two separate investigations into DEA's use of two Amtrak employees and one TSA employee as sources. These investigations determined the DEA's use of these individuals as sources was improper.[1] During this audit, we found that, between FYs 2011 and 2015, the DEA actually used at least 33 Amtrak employees and 8 TSA employees as sources, paying the Amtrak employees over $1.5 million and the TSA employees over $94,000. Indeed, even after we issued our investigative reports detailing our findings of improprieties, the DEA continued to use seven Amtrak employees as sources. The continued use of these sources only ceased in March 2016 when the DEA Inspections Division mandated that the field offices deactivate the seven sources and the DEA promulgated an interim policy

[1] See the summaries of the investigations' findings on our website: *Investigative Summary of Findings Concerning the DEA's Use of Amtrak Employees as Paid Confidential Sources* (January 2016) and *Investigative Summary of Findings Concerning the DEA's Use of a TSA Airport Security Screener as a Paid Confidential Source* (January 2016).

with a highly specific prohibition on using government or quasi-government employee sources (to include contract employees) to obtain information within the scope of their official duties. The DEA formalized this policy in July 2016.

We also found the DEA did not appropriately track all confidential source activity; did not document proper justifications for all source payments; and, at times, did not adequately safeguard traveler information. For example, Agents told us that they generally received tips from sources almost daily via email or text, some of which were sent to non-government private accounts established by the Agents, thereby possibly compromising travelers' personally identifiable information, affecting record maintenance requirements, and complicating the DEA's efforts to manage and access important case-related information. We also learned the DEA generally maintains confidential source tip information only when a consensual encounter and subsequent search leads to an arrest or seizure, and even then the information retained only pertains to the encounter. Because DEA's files do not detail the universe of information provided by its sources, it is unable to examine their reliability and whether they frequently or rarely provide useful information, or whether the information DEA agents acted upon resulted in identifying individuals involved in illegal activity or instead caused DEA to regularly approach innocent civilians for questioning.[2] We are deeply concerned about this inability to assess source reliability, which seriously impairs DEA's ability to oversee and manage the activity of these sources and the Confidential Source Program overall. We also found that Agents do not always include in DEA investigative reports references to confidential source information. Agents in one field office told us they do not do so because they hope to minimize exposure of the source. We believe the failure to document all source activity presents challenges to the tracking and retrieving of such activity, and therefore could increase the risk that some information relating to sources may not be available to prosecutors when needed in legal proceedings.

Additionally, we were extremely concerned to discover the DEA condoned its confidential sources' use of "sub-sources," who are individuals a source recruits and pays to perform activities or provide information related to the source's work for the DEA. During our review of DEA files, we found evidence of sources who were paid based, in part, on the need to pay "sub-sources," but the information in the files was insufficient to allow us to determine the full extent of such payments. We found that the DEA has no controls, policies, or procedures for interactions with these "sub-sources." Condoning the use of "sub-sources" to assist in investigations without the DEA's full knowledge, awareness, and approval raises serious questions – it increases the chance that individuals may be conducting unauthorized illegal activity on the DEA's behalf, potentially puts these and other individuals in harm's way, exposes the DEA and DOJ to significant liability, and could impact

---

[2] We identified a similar issue in our report on *The DEA's Use of Cold Consent Encounters at Mass Transportation Facilities* (January 2015), which found the DEA only retained data on consensual encounters when it led to a consensual search that resulted in a seizure or arrest, and therefore the DEA could not assess whether encounters were being conducted in an unbiased or effective manner.

prosecutions. We believe the DEA needs to evaluate whether "sub-source" use is appropriate and, if so, must develop policies and procedures to regulate it.

Another significant area of concern is the limited management, oversight, and tracking of source payments by the DEA's Intelligence Division, which oversees several programs under which sources provide information or conduct narcotics-related intelligence-gathering activities. According to DEA officials, the sources are used primarily for law enforcement purposes and the DEA's Intelligence Division generally relies on DEA field offices' risk assessments and determinations that confidential sources are reliable. In comparison, within the Executive Branch's Intelligence Community, of which the DEA's Office of National Security Intelligence is a member, there are standards for the appropriate handling of sources, including independent validation of sources. However, the DEA does not independently validate the credibility of sources used for intelligence programs or the accuracy of the information they provide. DEA legal and intelligence officials expressed concern over applying the Intelligence Community's validation and rating process to DEA's confidential sources because they believe it would impact the ability of prosecutors to effectively utilize DEA sources during narcotics-related criminal proceedings. We believe independent assessments of sources are critical to intelligence-gathering operations, and that relying on field offices to make these judgments without sufficient oversight from the Intelligence Division could negatively affect the Intelligence Division's ability to understand and appropriately use the information it receives.

Additionally, when we asked the DEA Intelligence Division to provide us with an itemized list and overall total of payments to intelligence-related confidential sources, it was unable to do so. We reviewed DEA records and estimated that, during the 5-year period of our review, the Intelligence Division paid more than $30 million to sources who provided narcotics-related intelligence and contributed to law enforcement operations, $25 million of which went to just 9 sources. Additionally, we identified one source who was paid over $30 million during a 30-year period, some of it in cash payments of more than $400,000. We concluded the Intelligence Division's management and oversight of its sources was not commensurate with the large amount of payments it made to them.

The deficiencies we identified in this audit raise significant concerns about the adequacy of the current policies, procedures, and oversight associated with the DEA's management of its Confidential Source Program. When we informed DEA management and program officials about our findings and concerns, these officials expressed a commitment to improve the DEA's Confidential Source Program, to implement appropriate controls over confidential sources, and to ensure that confidential sources remain a productive and essential element used by the DEA to accomplish its mission. This report makes several recommendations to help the DEA address deficiencies in its Confidential Source Program, and ensure that its handling of and payments to sources are appropriate, accountable, and reflective of the importance of, and risks posed by, its use of confidential sources.

AUDIT OF THE DRUG ENFORCEMENT ADMINISTRATION'S MANAGEMENT AND OVERSIGHT OF ITS CONFIDENTIAL SOURCE PROGRAM

TABLE OF CONTENTS

INTRODUCTION 1

Previous OIG and GAO Reports 1

DEA's Confidential Source Program Overview 3

DEA Confidential Source Categories and Payment Types 4

Confidential Source System Concorde 6

OIG Audit Approach 8

AUDIT FINDINGS 10

LIMITED USE CONFIDENTIAL SOURCE INVOLVEMENT IN DEA INTERDICTION ACTIVITIES 10

Limited Use Confidential Sources 10

Utilization of Limited Use Confidential Sources for Interdiction Activities 12

Amtrak Confidential Sources 14

Transportation Security Administration Employees 16

Commercial Airline Employees 17

Bus Transportation Employees Used as Confidential Sources 19

Parcel Company Employees as Confidential Sources 20

Significant Concerns and Legal Implications 22

Direction to Limited Use Confidential Sources 23

Tracking and Handling of Confidential Source "Tips," and the Consequences for Subsequent Discovery Obligations 25

Extensive Reliance on Limited Use Confidential Sources 27

THE DEA INTELLIGENCE DIVISION'S OVERSIGHT OF CONFIDENTIAL SOURCE ACTIVITIES AND THE DEA'S USE OF SUB-SOURCES 29

DEA Intelligence Division's Confidential Source Payments and Utilization 29

Confidential Source Validation 30

Intelligence Division Oversight of Confidential Source Payments 32

The DEA's Use of Sub-Sources in Enforcement and Intelligence Activities... 33

DEA CONFIDENTIAL SOURCE OVERSIGHT AND MANAGEMENT..... 35

Confidential Source Program Oversight Responsibilities 36

Confidential Source Categorization and Use Inconsistencies 37

Application of Confidential Source Category Based on Criminal History 37

Payments to Deactivated Confidential Sources..... 39

Confidential Source System Concorde Use and System Deficiencies..... 40

Payment Oversight and Management 42

Payment Tracking Discrepancies 42

Payment Support and Documentation Discrepancies 44

CONCLUSION AND RECOMMENDATIONS..... 46

STATEMENT ON INTERNAL CONTROLS..... 49

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS..... 50

APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY 51

APPENDIX 2: THE DRUG ENFORCEMENT ADMINISTRATION'S RESPONSE TO THE DRAFT AUDIT REPORT 54

APPENDIX 3: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT 59

AUDIT OF THE DRUG ENFORCEMENT ADMINISTRATION'S MANAGEMENT AND OVERSIGHT OF ITS CONFIDENTIAL SOURCE PROGRAM

INTRODUCTION

This is the second and final report resulting from the Department of Justice (DOJ or Department) Office of the Inspector General's (OIG) audit of the Drug Enforcement Administration's (DEA) Confidential Source Program that was initiated in February 2014. In July 2015, the OIG issued an audit report associated with this review to report on significant issues we had identified at that time.[3] However, due to obstacles and delays imposed by the DEA on the OIG's access to information necessary to our audit that lasted for over a year after we initiated the review, we were not able to report on our larger objective at that time. Since the issuance of our July 2015 report, the OIG has coordinated with the DEA and received its cooperation in our continued efforts to assess the DEA's management and oversight of its Confidential Source Program. We have now completed our review of the DEA's oversight of payments to confidential sources, evaluated compliance with pertinent rules and regulations associated with the use of confidential sources, and examined confidential source management practices employed by DEA domestic field offices and the DEA's Intelligence Division.

Previous OIG and GAO Reports

The OIG issued an audit report in 2005 that assessed the DEA's compliance with regulations concerning confidential informants and the DEA's controls over confidential source payments.[4] That audit identified several areas for the DEA to improve its management of the use of confidential sources to address findings regarding the DEA's failure to independently review and evaluate underlying suitability data, lack of proper documentation, failure to perform required reviews, instances wherein multiple DEA offices categorized the same source differently, as well as the improper categorization of other sources. Furthermore, the DEA did not adequately track receipts for reimbursements. The audit also concluded that the DEA did not have an effective system to account for and reconcile all confidential source payments.

More recently, the OIG's July 2015 report identified that the DEA's confidential source policy was not consistent with the Attorney General's Guidelines

---

[3] U.S. Department of Justice Office of the Inspector General, *Audit of the Drug Enforcement Administration's Confidential Source Policies and Oversight of Higher-Risk Confidential Sources*, Audit Report 15-28 (July 2015).

[4] U.S. Department of Justice Office of the Inspector General, *The Drug Enforcement Administration's Payments to Confidential Sources*, Audit Report 05-25 (May 2005).

Regarding the Use of Confidential Informants (AG Guidelines).[5] The AG Guidelines provide guidance to all Justice Law Enforcement Agencies (JLEA), including the DEA, related to establishing, approving, utilizing, and evaluating confidential sources. In addition, we determined that the DEA did not have adequate policies and practices for reviewing, approving, and revoking confidential sources' authorization to conduct Otherwise Illegal Activity (OIA). Further, the DEA was not conducting the required assessment of long-term or other confidential sources in a timely or adequate manner.[6] The report also noted that the DEA Special Agents Manual lacked directives related to recruiting, establishing, and using confidential sources that are subject to DEA regulatory requirements. The report additionally identified significant concerns regarding the DEA's provision of *Federal Employees' Compensation Act* (FECA) benefits to confidential sources. In response to this report, the DEA has coordinated with the Criminal Division and developed updated Confidential Source Program policies to comply with the AG Guidelines; the DEA's updated confidential source policies were officially incorporated into DEA operations in July 2016. In addition, the DEA has implemented new policies and procedures related to the provision of FECA benefits to confidential sources.

In January 2016, the OIG made public summaries of its findings in two investigations related to the DEA's use of Amtrak and Department of Homeland Security (DHS) Transportation Security Administration (TSA) employees as paid confidential sources.[7] The OIG determined that the DEA paid two Amtrak employees more than $860,000 for information that was available at no cost to the government in violation of federal regulations relating to the use of government property, thereby wasting substantial government funds. Similarly, the OIG found that by registering a TSA Security Screener as a confidential source, the DEA agreed to pay for information that the screener was already obligated to provide to law enforcement. In both of these investigations, the OIG determined that the DEA violated or exceeded the terms of its confidential source policies.

Finally, the Government Accountability Office (GAO) issued a report in September 2015 on DOJ and Department of Homeland Security (DHS) law enforcement components' confidential informant policies. GAO's report identified that the DEA did not have policies that were fully consistent with the AG

---

[5] Following the issuance of the July 2015 OIG report, DOJ officials from the Office of the Deputy Attorney General (ODAG), Criminal Division, and DEA coordinated to improve the DEA's policies related to the management and use of confidential sources to ensure that the policies contain all requirements included within the AG Guidelines.

[6] The DEA does not have a unique category for long-term confidential sources, but it does use this term (outside of its DEA Special Agents Manual) and identifies these individuals as sources active for 6 or more consecutive years.

[7] U.S. Department of Justice Office of the Inspector General, *Investigative Summary of Findings Concerning the DEA's Use of Amtrak Employees as Paid Confidential Sources* (January 2016), and U.S. Department of Justice Office of the Inspector General, *Investigative Summary of Findings Concerning the DEA's Use of a TSA Airport Security Screener as a Paid Confidential Source* (January 2016).

Guidelines.[8] Specifically, the report stated that DEA policy was not consistent with the requirements to provide written instructions to informants regarding the parameters of authorized Otherwise Illegal Activity and to have informants sign an acknowledgment of these instructions.[9]

DEA's Confidential Source Program Overview

The DEA defines a confidential source as any person who, with a reasonable expectation of confidentiality, furnishes information regarding drug trafficking, or performs an investigative activity. The DEA uses confidential sources throughout the world to assist in investigating criminal activity and to regularly contribute information to the DEA.

As we identified in our July 2015 audit, DEA officials believe that the DEA could not effectively enforce the controlled substances laws of the United States without the use of confidential sources. These officials conveyed that confidential sources play a significant role in DEA's processes for initiating investigations and providing DEA with invaluable information and services that facilitate arrests and seizures of drugs and currency. However, confidential sources can be motivated by many factors, including fear, financial gain, avoidance of punishment, competition, and revenge; therefore, special care must be taken to carefully evaluate and closely supervise their use. Moreover, the credibility and the appropriate and legal use of confidential sources must always be considered and balanced against the information and services they provide.

The DEA's Office of Operations Management administers the Confidential Source Program through the Confidential Source Unit. This Unit provides support to the field and manages the electronic system that maintains data on each confidential source – the Confidential Source System Concorde (CSSC). However, the DEA relies on its field office personnel to recruit, manage, direct, and evaluate the use of confidential sources.

DEA Special Agents in field offices establish, utilize, control, and pay confidential sources. Supervisory personnel must review and approve all confidential source activities and payments. Both Special Agents and supervisory personnel are responsible for documenting these activities and payments in the confidential source files and in CSSC. Each field office is also assigned a Confidential Source Coordinator who must provide guidance to Special Agents and supervisory personnel regarding aspects of the Confidential Source Program.[10] The

---

[8] GAO, *Confidential Informants Updates to Policy and Additional Guidance Would Improve Oversight by DOJ and DHS Agencies,* GAO-15-807, (September 2015).

[9] The AG Guidelines allow JLEAs to authorize confidential sources to engage in activity that would otherwise be illegal if they were not acting under the direction of the government.

[10] Both DEA Special Agents and Task Force Officers manage DEA confidential sources; however, in this audit report we use "Special Agent" to refer to both DEA Special Agents and DEA Task Force Officers.

Confidential Source Coordinator is also responsible for maintaining the integrity and completeness of information stored in CSSC and the confidential source files. The integrity and completeness of confidential source files are reviewed during the annual self-inspections process, which is conducted by each field office and submitted to the DEA Inspections Division. To complement the self-inspections process, the Inspections Division also conducts on-site reviews of each field office, including Confidential Source Program activities, at each field office on a 4 to 5-year cycle.

Finally, although the majority of the DEA's confidential sources are established and used by its field offices, the DEA's Intelligence Division also utilizes confidential sources to advance intelligence-related operations and programs. The Intelligence Division's role in using, and the supervision of, confidential sources is described in detail later in this report.

DEA Confidential Source Categories and Payment Types

The DEA has established categories for confidential sources with different handling requirements, and with different levels of approval and scrutiny of confidential source use. Table 1 describes the DEA's confidential source categories.

Table 1

Overview of DEA Confidential Source Categories as Defined by the DEA Special Agents Manual

Categories	Definitions
Regular Use	A confidential source who does not meet the criteria for establishment as a Restricted Use, Defendant, or Protected Name confidential source.
Restricted Use	A confidential source who will be subject to a greater degree of supervisory control based upon factors within his/her background that indicates a need for such supervision.
Limited Use	A confidential source who is established as a confidential source for payment purposes only and who is a "professional" businessperson or a "tipster."
Defendant	A confidential source who was under arrest or is subject to arrest and prosecution for a federal or state offense; requires federal or state prosecutor concurrence for establishment.
Protected Name	A confidential source whose public identification or utilization as a DEA confidential source could pose a threat to the national security of the United States or a foreign country, or result in a high likelihood of violence to the confidential source and/or his/her family members or associates, or is likely to raise complex legal issues.

Source: DEA Special Agents Manual

The DEA's primary purpose for establishing these categories is to distinguish the different levels of oversight for the sources, including variant supervisory and outside approval and reporting requirements based on the level of risk associated with the source. As identified in Table 2, the DEA's requirements for Restricted Use, Defendant, and Protected Name sources are the most stringent and provide for additional oversight, while the requirements for Limited Use confidential sources

are less stringent and do not necessitate extensive oversight. Compared to the other confidential source categories, the annual review requirements for Limited Use confidential sources are considerably reduced. Specifically, if an individual meets the DEA's criteria for a Limited Use confidential source, completion of the risk assessment is not required and limited information related to the office designator, activation, source type, payment totals, and criminal history is identified on an annual suitability form. In some instances, and with additional approval, DEA Special Agents can establish individuals as both Defendant and Restricted Use if they meet the criteria.

Table 2[a]

DEA Confidential Source Category General Requirements

		Confidential Source Categories				
		Restricted Use	Defendant	Protected Name	Regular Use	Limited Use
Initial Approval Requirements	Group Supervisor	✓	✓	✓	✓	✓
	Assistant Special Agent in Charge	✓	✓	✓		
	Special Agent in Charge	✓[b]		✓		
	Prosecutor (Concurrence)		✓			
Reporting Requirements	Initial Debriefing & Risk Assessment	✓	✓	✓	✓	
	Fingerprints & Photographs	✓	✓		✓	
	Quarterly Debriefings	✓	✓	✓	✓	
	Annual Debriefing & Risk Assessment	✓	✓	✓	✓	✓

[a] The requirements depicted in this chart are based on the DEA's confidential source policy that was in effect during our audit. In response to our July 2015 report, the DEA formally implemented policy changes in July 2016.

[b] Approval by the Special Agent in Charge to establish a Restricted Use confidential source is required in a limited number of specific circumstances, such as establishing a federal prisoner as a confidential source. In other cases, Special Agent in Charge approval for Restricted Use sources is discretionary and based on the assessment and recommendation of the Assistant Special Agent in Charge.

Source: OIG Analysis of DEA Special Agents Manual and DEA Annual Continuing Suitability Report and Recommendation

As part of their working relationship with the DEA, the confidential sources may receive check or cash payments from the DEA for their DEA-related activities. These payments are attributed to various categories and purposes, as outlined in Table 3.

Table 3

Overview of DEA Confidential Source Payment Types as Defined by the DEA Special Agents Manual

Categories[a]	Definitions and Approvals
Services/Information	A confidential source may be compensated for services or information during any stage of the investigation in which the confidential source provides covert assistance to DEA.
Award	Payments of up to $500,000 or 25 percent of the amount realized by the government from asset forfeiture, whichever is less, for information or assistance leading to a civil or criminal forfeiture. A confidential source must have provided original information that clearly led to asset forfeiture. A payment under this provision shall preclude the confidential source from receiving any additional Assets Forfeiture Fund awards based on the same information.
Reward	A confidential source may receive a reward payment from operational funds upon the culmination of the covert stage of an investigation. This payment may be made from operational funds even if the confidential source has been recommended for Assets Forfeiture Fund awards.
Reimbursement for Expenses	Confidential sources can be compensated for reasonable expenses incurred during investigation. The expenditure of funds for this purpose must be documented. Receipts will be obtained from the confidential source whenever possible. The receipts will be attached to payment documents and filed in the confidential source file.
Relocation	DEA may fund confidential source expenses for relocation for security purposes. These expenses may include travel for the confidential source and his or her immediate family, movement and/or temporary storage of household goods, and temporary living expenses at a new location for a period of time not to exceed six months.
Security	DEA may be required to provide security assistance to a confidential source that does not entail the relocation of the confidential source.

[a] Payments for the Purchase of Evidence, Payments from Trafficker Directed Funds, and Special Payments are also confidential source-related payments. However, the payments to confidential sources reviewed during this audit were primarily those in Table 3 above.

Source: DEA Special Agents Manual

Confidential Source System Concorde

As mentioned, the DEA uses CSSC to track, manage, and record confidential source related information.[11] CSSC is a web-based application and is an electronic repository for confidential source-related investigative reports, payments, and other

[11] The DEA Special Agents Manual and Confidential Source Program officials state that the confidential source paper files are the official record for confidential sources.

documents specific to individual confidential sources. CSSC is linked to both the Unified Financial Management System (UFMS), in order to track payments made to confidential sources, and the DEA's case system, in order to track cases in which the confidential source is involved.

During the audit, the OIG obtained and analyzed CSSC data related to confidential sources who were ever active in any DEA domestic office between fiscal years (FY) 2011 and 2015. We determined that due to weak internal system controls the data entered into the system was not always accurate, consistent, or complete. Moreover, we found that certain DEA processes to pay sources resulted in missing data related to source payment information. As a result, although we used the data to identify certain risk indicators during our sample selection of field office confidential source files, we did not rely on the data to make conclusions and recommendations regarding significant deficiencies without validating with other documentation. The weaknesses we identified in CSSC and our use of CSSC data are discussed in further detail in the DEA Confidential Source Oversight and Management section of the report and Appendix 1.

Because it was the only Confidential Source Program data available, we used CSSC data within our findings about specific confidential sources or source types. These results are used for informational purposes related to our audit findings, as well as general programmatic information for DEA's review. Table 4 provides an overview of the number and total payments to confidential sources from FY 2011 through FY 2015 based on our analysis of CSSC data.

Table 4

FY 2011 through FY 2015
Universe and Payments by Source Type

Confidential Source Category	Number of Active Confidential Sources	Number of Paid Confidential Sources[a]	Payment Totals[b]
Regular Use	4,566	2,840	$77,884,545
Restricted Use	5,458	3,470	52,404,859
Limited Use	699	477	26,808,549
Defendant	6,144	1,383	3,238,711
Protected Name	72	39	3,341,216
Multiple Categories[c]	1,786	1,330	73,805,868
Special Payment[d]	1	1	5,000
Total	**18,726**	**9,540**	**$237,488,748**

[a] Not all active confidential sources received payments. The number of paid sources is a subset of the number of active sources.

[b] Payments generally consist of amounts paid from DEA appropriated and non-appropriated funds such as the High Intensity Drug Trafficking Area Program, as well as award amounts paid from the Assets Forfeiture Fund and other reward programs.

[c] These sources encompass those whose category changed during our review period or who were used concurrently by offices that applied different categories for the same source.

[d] Special Payment is comprised of only one record that did not have a corresponding category as defined by the DEA Special Agents Manual.

Source: OIG analysis of DEA CSSC Data

OIG Audit Approach

To accomplish our objective, we conducted more than 50 interviews with Department and DEA headquarters officials, as well as field office Special Agents and Task Force Officers. In addition, we conducted site visits at the DEA's offices in Chicago, Illinois; San Francisco and Sacramento, California; El Paso, Texas; Phoenix, Arizona; Albuquerque, New Mexico; and Los Angeles, California; as well as the DEA's Office of Special Intelligence and the Special Operations Division. During these site visits, we reviewed 120 confidential source files and 19 investigative case files. The sources we reviewed were paid over $36 million during our review period. Finally, we reviewed DEA Inspections Division reports, analyzed DEA documentation, and reviewed OIG reports of investigations.

This audit focuses on the DEA's management and oversight of its Confidential Source Program, to include the DEA's oversight of payments to confidential sources. Our results are organized into three findings focused on the following areas: Limited Use confidential sources used in interdiction-related activities; confidential sources associated with DEA Intelligence Division programs; and DEA's oversight

and management of its Confidential Source Program. Additional information about our approach to this audit is in Appendix 1.

AUDIT FINDINGS

LIMITED USE CONFIDENTIAL SOURCE INVOLVEMENT IN DEA INTERDICTION ACTIVITIES

Limited Use confidential sources, as described by DEA officials, provide independent and lawfully obtained information, or "tips," to the DEA and require the least amount of supervision and oversight. We found that DEA's interdiction activities rely on Limited Use confidential sources who are travel and parcel industry employees. During our review of 53 confidential source files associated with 6 different DEA field offices conducting interdiction activities, we found that the DEA paid these sources approximately $4.6 million between FY 2011 and FY 2015. The majority of these 53 sources were paid to conduct searches on proprietary databases, or access packages shipped through private companies, to provide traveler and package information to the DEA to assist in interdiction activities.

We found the DEA has not provided sufficient oversight in the establishment, use, and payment of these sources by DEA's Interdiction Units. As a result, the DEA improperly established a TSA employee as a Limited Use confidential source and inappropriately paid Amtrak employees for information that could have been obtained at no cost to the DEA. In addition, we found that the DEA routinely did not document all of its interactions with sources or adequately handle and secure the proprietary, potentially personally identifiable information obtained from confidential sources. Finally, we found that the DEA's direction and guidance to its Limited Use sources, its reliance on sources to accomplish its interdiction mission, and its sometimes long-term and lucrative relationships with these sources calls into question whether the source is truly providing information independently or is acting as DEA's agent, the latter of which could have implications relating to compliance with the Fourth Amendment's protections against unreasonable searches and seizures.

Limited Use Confidential Sources

According to the AG Guidelines, a Source of Information is an individual who meets the definition of a confidential informant and 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, and not as a result of criminal association with persons of investigative interest to the JLEA; and provides such information in a manner consistent with applicable law. The AG Guidelines requirements do not apply to Sources of Information.

The DEA identifies this category of persons in the DEA Special Agents Manual as Limited Use confidential sources. According to the DEA Special Agents Manual, to assign a confidential source to the Limited Use category, the following must be established:

1. The person may be recruited by DEA, but must provide information independently (without direction by DEA).
2. This person would not be required to testify as a witness in any legal proceeding. In other words, DEA could independently corroborate the information supplied by the confidential source.
3. DEA anticipates rewarding this person for information/services rendered.
4. The information obtained by this person is not provided because of criminal association with persons of investigative interest to the DEA.

According to the DEA Special Agents Manual, the role of the Limited Use confidential source is only to provide information that has been independently and lawfully obtained, and is of investigative interest to the DEA. Additionally, the Limited Use category (as shown in Table 2) is regarded by DEA as low-risk and has fewer controls and levels of supervision needed to approve establishment, use, and payments to these sources.

During our review of CSSC data, we observed that Limited Use confidential sources were some of the highest paid DEA confidential sources. Specifically, our analysis of the universe of confidential source payments during the period of our review identified that the 477 confidential sources categorized and paid solely as Limited Use received over $26.8 million (as shown in Table 4), or an average of over $56,000 per source. From our initial review of a sample of confidential source files and interviews with handling agents, we learned that the DEA often used Limited Use confidential sources to assist with DEA interdiction activities that occur at airports, train and bus stations, and parcel companies. For example, the DEA established employees of transportation and parcel companies as confidential sources. We reviewed documentation related to payments made to these confidential sources and found that the information and services provided by these Limited Use confidential sources, some of whom have government affiliations – such as Amtrak and TSA employees – resulted in seizures of currency, forfeiture cases, seizures of drugs, and arrests.[12] We identified several significant areas of concern related to the DEA's use of these Limited Use confidential sources for its interdiction-related activities.

[12] Amtrak is considered a quasi-government organization because it is a partially government-funded American passenger railroad service. The Amtrak Board of Directors sets policy and oversees the management of the company and includes seven members appointed by the President of the United States with the advice and consent of the Senate.

Utilization of Limited Use Confidential Sources for Interdiction Activities

To carry out its mission to enforce the controlled substances laws and regulations of the United States, the DEA established Interdiction Units to "effectuate seizures of illegal drugs and illegal drug proceeds." To accomplish this goal, these Interdiction Units conduct consensual encounters with, and searches of, members of the public.[13] We reviewed 53 confidential source files associated with 6 different DEA field offices conducting interdiction activities, hereafter referred to as Interdiction Units, and interviewed 13 Special Agents who utilized confidential sources for interdiction-related activities. We found that Special Agents who work interdiction operations recruit individuals employed in the travel industry, including airlines, Amtrak, bus companies, and parcel facilities, to become confidential sources. Specifically, Special Agents stated that they identify employees who have access to traveler databases or who interact with travelers on a regular basis and can provide the DEA with "real-time" information. The DEA also recruits individuals who work in the parcel industry and have access to package facilities and shipment databases or records and can provide the DEA with information. The DEA establishes these individuals using the Limited Use confidential source category because, according to the Special Agents Manual and DEA Agents, the DEA does not use these confidential sources in operations to buy drugs and does not rely on them for their knowledge, involvement, and association with criminal activity.

To recruit and establish travel and parcel industry employees as confidential sources, Special Agents identify, or may be approached by, individuals who are willing to participate in a working relationship with the DEA. According to Special Agents, when these "professional" Limited Use confidential sources are established, the DEA uses the expertise of Special Agents to instruct the sources on what constitutes suspicious travel or suspicious parcels with the intent of having the sources identify these suspicious activities in company databases or identify suspicious passengers, luggage, or packages en route. Special Agents from the Interdiction Units stated that they tell these individuals that, as confidential sources, the DEA may compensate them for the information provided and they may receive monetary awards if their information results in seizures and subsequent forfeitures. According to some of these DEA Special Agents, Limited Use confidential sources generally agree to work with the DEA because of the prospect of receiving significant financial awards.

Once these confidential sources have an understanding of the DEA's "suspicious" criteria, they can make ongoing observations while conducting their general employment activities. However, many of the highly paid confidential sources we reviewed also conducted active searches of travel databases or physical searches of parcel facilities for the purpose of providing the DEA with traveler

---

[13] According to the DEA Interdiction Manual, the DEA conducts interdiction operations at major transportation facilities to detect and stop, or at least deter movement of drugs through conventional means of transportation. In January 2015, the OIG issued a report on *The DEA's Use of Cold Consent Encounters at Mass Transportation Facilities*, Evaluation and Inspections Division Report 15-3.

itineraries and parcels. According to Special Agents, the number of tips and amount of information contained in each tip may vary by source, but in general, these tips are the initial foundation of many DEA interdiction events because they are a more effective starting point than a "cold" consensual encounter. In fact, Special Agents we interviewed from the 6 DEA Interdiction Units we reviewed estimated that 70 to 100 percent of all of their consensual encounters were initiated because of Limited Use confidential source tips.

After travel itinerary-related tips are received, if time allows, Special Agents or Intelligence Analysts perform a brief background investigation to research the passenger information included in the tip. The explanation of this process varied slightly among Interdiction Units, but generally, Special Agents described that the brief investigation includes a background check to prioritize the confidential source tips and to select the most ideal passengers for consensual encounters. However, according to these Special Agents, if time does not allow, they could use the tip as the basis for encountering a passenger who does not have any criminal background association. These brief investigations are time sensitive because the information provided by the confidential sources is often regarding passengers who are already en route to or departing the Special Agents' location.

Similarly, Special Agents from Interdiction Units stated that for parcel-related tips, they may perform a brief background check on parcel senders and recipients, if time allows for it. We found that Special Agents use the tip to track packages based on sender and receiver information and to intercept packages en route in order to conduct controlled deliveries of suspicious packages and to perform subsequent consensual encounters with the sender and/or receiver.

If during a consensual encounter and subsequent search the DEA finds a person transporting illegal substances, it seizes the drugs and arrests the person. If the DEA finds currency, Special Agents must make a determination, based on various investigative criteria, whether the currency is related to suspected drug proceeds and if the government should seize it. If a consensual search results in currency being seized from someone as suspected drug proceeds, the currency is processed through the asset forfeiture program and, unless contested, will be deposited into the Assets Forfeiture Fund.[14] The Special Agents we spoke to stated that the funds seized during interdiction cases and consensual searches are vital in dismantling drug organizations. The Special Agents also stated that by focusing on money seizures the DEA may effectively shut down a drug trafficking organization because drug proceeds represent the culmination of the organization's efforts.

---

[14] The DOJ Asset Forfeiture Program encompasses the seizure and forfeiture of assets that represent the proceeds of or were used to facilitate federal crimes. The Assets Forfeiture Fund was established to receive the proceeds of forfeitures and to pay the costs associated with the costs of such forfeiture. The Attorney General is authorized to use the fund to pay any necessary expenses associated with forfeiture operations, to include the payment of awards for information or assistance leading to a civil or criminal forfeiture. The OIG is conducting a review that is examining DOJ's asset seizure and forfeiture activities from FY 2007 to FY 2014, with particular attention paid to the forfeiture of seized cash, and reviewing the effects of recent DOJ policy limiting the ability of DOJ agencies to adopt assets seized under state law.

In the case of both drug and currency seizures, DEA Special Agents may request that the confidential source who provided the initial tip receive a monetary award for their contributions to DEA cases. For seizures of currency and other items of value, the award can be up to 25 percent of the amount realized from the asset forfeiture, but no more than $500,000. For seizures of drugs or other contraband, there is no formal guidance on the establishment of award amounts.

While Limited Use confidential sources used in the DEA's interdiction-related activities provide similar types of information, we found differences in the DEA's handling and use of these confidential sources. These differences were largely dependent upon the industry toward which the field office focused its interdiction efforts. A more detailed look at the DEA's use of confidential sources in the Amtrak, TSA, commercial airline, intercity bus company, and parcel industries is provided below, by type.

Amtrak Confidential Sources[15]

We found that from FY 2011 through FY 2015, the DEA established, utilized, and/or paid at least 33 Amtrak employees as Limited Use confidential sources.[16] Based on our analysis of the DEA's CSSC data, we estimated that the DEA paid these employees over $1.5 million between FY 2011 and FY 2015, and appears to have paid them more than $2.3 million historically.[17]

These Amtrak employees included train attendants who could identify passengers and their luggage, and ticket agents who could query the Amtrak passenger name records (PNR) system to provide the DEA with passenger travel reservations. According to Special Agents, the PNRs provided to the DEA by these confidential sources are computerized printouts of a passenger reservation and are selected by the confidential source based on DEA-developed indicators of suspicious travel such as tickets purchased last minute, tickets purchased with cash, and travel to and from drug trafficking source cities.[18] The PNR information we reviewed generally included passenger name, origin and destination cities, trip

---

[15] We have coordinated with the Amtrak OIG on our identification of the DEA's use of Amtrak employees as confidential sources.

[16] We identified 33 confidential sources who were employed by Amtrak. We identified these individuals by reviewing multiple fields in the CSSC data and looked for different variations of spelling Amtrak or occurrences of the word "railroad." However, despite our search, due to the various methods DEA employees used to input this employer information, there remains the potential that we did not identify all Amtrak employees who were used as confidential sources by the DEA.

[17] This historical amount was based upon our analysis of CSSC data, which included historical payment information as far back as 1992 for these Amtrak confidential sources. As these payments were prior to our review period, the OIG did not reconcile historical payments found in CSSC to documentation in the confidential source file to verify or validate the historic payment information.

[18] Through its investigations and other significant information, the DEA has identified numerous cities as "source cities" for narcotics, which is one indicator used to evaluate the risk of narcotics trafficking and narcotics proceeds trafficking.

itinerary, seat and train car numbers, as well as information related to the purchase of the fare including whether the purchase was made with cash or credit and whether the purchase was made via the telephone or internet. Although we could not review any PNR documentation because it was not maintained in the confidential source files we reviewed, Special Agents told us that confidential sources sometimes also provide passenger dates of birth.

We interviewed DEA Special Agents who used Amtrak ticket agents as confidential sources. These agents told us that these sources provided the DEA with PNR information on a daily basis via email, text, or telephone call. As described above, if the Special Agents have time, they will perform a brief background investigation on the passengers associated with the tips in an attempt to identify passengers with narcotics violations and criminal associations. These Special Agents used the Amtrak tip information to conduct consensual encounters and searches with the goal of seizing currency deemed narcotics proceeds and illegal substances, and making related arrests.

We performed a detailed review of 21 of the 33 Amtrak sources we identified. Our review included an in-depth examination of the DEA confidential source file, interviews with handling agents, and reviews of certain case files. Table 5 gives an overview of the Amtrak employee Limited Use confidential sources included in our review.

Table 5

FY 2011 to FY 2015
21 Amtrak Employee Confidential Sources
Reviewed by the OIG

Confidential Source File Information Reviewed	Totals
Sources Tested	21
Number of Payments to Tested Sources	175
Amount Paid to Sources	$1,397,168
Cases	170
Total Currency Seized	$7,548,204
Number of Instances an Illegal Substance was Seized	72

Source: OIG analysis of DEA confidential source files

As previously mentioned, in January 2016, the OIG released a summary of its findings relating to its investigation involving two Amtrak employees recruited as confidential sources to provide the DEA with information. The investigation found that the information reported by Amtrak employees who were established as confidential sources could have been obtained by DEA at no cost through a joint task force with the Amtrak Police Department (APD). However, as of January 2014, the OIG determined that over a period of 20 years, the DEA paid one of the Amtrak employees $854,460 for PNR information, which was a substantial waste of

government funds. The DEA paid the other Amtrak employee $9,701. In this audit, we further determined that, according to the DEA's CSSC data, the confidential source who was paid $854,460 through January 2014 received an additional $108,155 between January 2014 and February 2015, thus increasing the total amount paid to this Amtrak employee to $962,615, of which $726,439 was paid during our review period.

Moreover, we determined that even after the OIG issued its Report of Investigation to the DEA in November 2015, the DEA continued to use Amtrak employees as Limited Use confidential sources; as of January 2016, the DEA had seven Amtrak sources still active. DEA Special Agents from two separate field offices justified the continued use of these confidential sources by saying Amtrak Detectives were often too busy and unable to provide PNRs to the DEA. In addition, these Special Agents stated that Amtrak confidential sources, who handle reservations as a matter of daily routine duties, were more proficient than Amtrak Detectives at searching the Amtrak system for PNRs.

According to the DEA, the use of these confidential sources ceased when, in March 2016, the DEA Inspections Division became aware that certain DEA field offices continued to use Amtrak employees as confidential sources after a field office submitted a confidential source establishment form for an Amtrak employee. The DEA's Confidential Source Unit identified this as an issue and elevated it to the DEA's Inspections Division, and the Confidential Source Unit did a subsequent query for all active Amtrak-employed confidential sources. Based on these results, the DEA Inspections Division mandated that three field offices deactivate the seven active Amtrak sources that had been identified. In addition, the DEA promulgated a highly specific interim policy in March 2016 that prohibits the establishment of government or quasi-government employees (and contractors) as sources, including Amtrak employees, in order to obtain information related to their official job responsibilities. This policy was formalized in July 2016.

Transportation Security Administration Employees[19]

We analyzed the DEA's CSSC data and reviewed confidential source documentation and found that between FYs 2011 and 2015, the DEA had approximately eight TSA employees, including security screeners, as active confidential sources, half of whom were categorized as Limited Use confidential sources.[20] According to CSSC, the DEA paid three of these confidential sources a total of over $94,000 during this time. Establishing, using, and paying these TSA

[19] We have coordinated with the Department of Homeland Security OIG on our identification of the DEA's use of TSA employees as confidential sources.

[20] Due in part to the aforementioned OIG investigation, we did not conduct any file reviews related to TSA confidential sources as part of this audit. Through our review of CSSC data, we identified eight confidential sources who were employed by TSA. However, due to the various methods DEA employees used to input this employer information into CSSC, combined with CSSC data integrity issues discussed later in this report, there remains the potential that we did not identify all DEA confidential sources who were also TSA employees.

employees as confidential sources for providing information obtained through their TSA positions violated DEA policy.

These findings are consistent with a prior OIG investigation, described in a January 2016 investigative summary that examined the DEA's establishment and use of a TSA security screener as a Limited Use confidential source. The DEA used the security screener to identify and provide the DEA with information pertaining to suspicious passengers carrying large sums of money that were identified during the course of the sources' TSA duties. The OIG's investigation found that registering a TSA security screener as a confidential source violated DEA policy, which precludes registering as a confidential source "employees of U.S. law enforcement agencies who are working solely in their official capacity with DEA." The OIG also found that TSA screeners are obligated to report to law enforcement suspected criminal activity that they observe in the course of their duties, therefore the DEA agreed to pay for information that the screener was already obligated to provide to law enforcement. Further, the OIG determined that asking the TSA screener to notify the DEA of suspicious activity in exchange for a possible monetary award violated the DEA's Interdiction Manual, and registering the TSA screener as a confidential source could have resulted in violations of individuals' constitutional protection against unreasonable searches and seizures if the TSA screener's actions led to subsequent DEA enforcement action.

As indicated above, in March 2016, the DEA promulgated an interim policy that clearly and specifically prohibits the establishment of all government or quasi-government employees or contractors, including TSA employees, as confidential sources to obtain information related to their official job responsibilities. Around this time, the DEA also provided the OIG with evidence that it had deactivated all eight TSA-employed confidential sources. This policy was formalized in July 2016.

Commercial Airline Employees

The DEA established, utilized, and paid commercial airline employees as Limited Use confidential sources.[21] When we initiated our audit, DEA officials used an airline employee as an example of a Limited Use confidential source and stated that based on their employment and common dealings with the passengers, these individuals may observe suspicious behavior or identify suspicious travel itineraries or luggage that they can report to the DEA. Thus, these types of individuals qualify as Limited Use confidential sources because they are not involved with criminal activity, are professional employees, and independently provide information to the

[21] We attempted to analyze the DEA's CSSC data to identify confidential sources who were employed within the airline industry, but due to the numerous types and large number of different entities involved in this industry, as well as the inconsistencies related to the various methods DEA employees used to input employer information into CSSC, we could not estimate with any certainty the universe of DEA confidential sources employed within the airline industry. Therefore, our results for this industry are strictly based on the universe of airline industry confidential sources whose files we reviewed.

DEA. During our review of six DEA Interdiction Units, we learned that many of these individuals were recruited by DEA Special Agents because they had access to corporate airline databases containing detailed passenger information. During our review of DEA confidential source files, we found that these Limited Use confidential sources provided DEA Special Agents with passenger travel information including itinerary information, ticket purchase information, baggage information, origin and destination airports, connecting flights, dates of birth, flight numbers, and seat numbers.

According to DEA Special Agents, these confidential sources send this type of passenger information, or "tip," to the DEA on a near daily basis via email, text, or telephone. Similar to the process used with Amtrak confidential sources, if time allows, Special Agents conduct a brief background investigation on the traveler information included in the "tip," otherwise the Special Agents rely on the "tip" as impetus for attempting a consensual encounter with the traveler. Successful encounters and consensual searches with commercial airline passengers result in the seizure of currency or illegal drugs. Because these interdiction encounters take place in airports, with higher security procedures than other modes of travel such as trains, it is less likely that illegal drugs will be found by the DEA. Therefore, the majority of monetary awards to airline employee confidential sources that we reviewed were received for a "tip" that led to a DEA currency seizure.

We performed an in-depth examination of 19 confidential source files associated with commercial airline employees. The DEA paid these 19 Limited Use confidential sources $1,615,232 during our review period, and CSSC indicates that they received a total of about $3 million since their establishment. These 19 confidential sources were paid for their contributions to 381 cases. The following table gives an overview of the commercial airline employee Limited Use confidential sources included in our review.

Table 6

FY 2011 to FY 2015
19 Commercial Airline Employee Confidential Sources Reviewed by the OIG

Confidential Source File Information Reviewed	Totals
Sources Tested	19
Number of Payments to Tested Sources	390
Amount Paid to Sources	$1,615,232
Cases	381
Total Currency Seized	$14,322,107
Number of Instances an Illegal Substance was Seized	2

Source: OIG analysis of DEA confidential source files

Of the confidential source files that we reviewed, we found variances in the level of the sources' activity with the DEA. According to Special Agents, some of these confidential sources are more proactive than others in searching for suspicious itineraries to provide to the DEA. These Special Agents elaborated that after receiving award payments, some confidential sources increase their search activity to provide more "tips" to the DEA in the hopes of obtaining additional payments. In one file we reviewed, we found that between October 2012 and July 2015, the DEA paid a Limited Use commercial airline employee confidential source approximately $617,676 related to "tips" associated with 130 different interdiction consensual encounter cases. The DEA paid the confidential source approximately 12 percent of the total amount seized.

Bus Transportation Employees Used as Confidential Sources

The DEA established, utilized, and paid as Limited Use confidential sources, private intercity bus company employees.[22] Generally, we found that bus transportation-related confidential sources were established and utilized by one of the six DEA Interdiction Units we visited. Special Agents explained to us that these individuals are used as confidential sources because they either worked on the buses and could provide DEA with information based upon the source's observations of suspicious passengers and luggage or because the sources had access to private bus company databases and could provide passenger itinerary information to the DEA. According to a DEA Special Agent who specializes in using these Limited Use confidential sources, he tries to find individuals who can use their access to the bus company database to obtain passenger manifests for buses en route. When this DEA Special Agent uses this type of confidential source, he requests that the source determine, and manually annotate on the manifest, passengers who purchased their fares with cash and send the entire manifest to the DEA via email. If time allows, the Special Agent will use the manifest provided to perform investigative background checks to determine the most ideal persons to engage for consensual encounters. Successful bus company-related consensual encounters and searches will result in the seizure of currency or illegal substances, and arrests.

We performed an in-depth examination of eight confidential source files associated with bus company employees. The DEA paid these 8 Limited Use confidential sources $383,112 during our review period and about $450,000 historically. The following table gives an overview of the private bus company Limited Use confidential sources included in our review.

[22] We attempted to analyze the DEA's CSSC data to identify confidential sources who were employed within the bus transportation industry, but due to the different entities involved in this industry, as well as the inconsistencies related to the various methods DEA employees used to input employer information into CSSC, we could not estimate with any certainty the universe of DEA confidential sources employed within the bus transportation industry. Therefore, our results for this industry are strictly based on the universe of bus transportation industry confidential sources whose files we reviewed.

Table 7

FY 2011 to FY 2015
Eight Bus Transportation Company Employee Confidential Sources Reviewed by the OIG

Confidential Source File Information Reviewed	Totals
Sources Tested	8
Number of Payments to Tested Sources	91
Amount Paid to Sources	$382,112
Cases	88
Total Currency Seized	$943,001
Number of Instances an Illegal Substance was Seized	67

Source: OIG analysis of DEA confidential source files

Of the eight bus company-employed confidential source files reviewed, we found that one bus company employee confidential source who provided the DEA with passenger manifests was paid more frequently and higher amounts than the other bus company sources. Specifically, between October 2012 and January 2016, this source provided the DEA, on an almost daily basis, the entire passenger manifest for buses traveling to or from a specific station of their private company employer. The DEA ultimately paid this Limited Use confidential source approximately $429,000 for the contributions to 99 interdiction-related cases.[23] In our judgment, the daily provision of an entire passenger manifest to the DEA is unlikely to align with the sources' legitimate and routine employer-assigned duties. Additionally, it would appear that the provision of this information does not require the confidential source to make any personal observation or conclusion. The source is simply using the employment position to procure and transfer private company manifests to the DEA, which then results in payment from DEA. We find the DEA's use of this confidential source particularly concerning because the DEA encouraged the source to provide the entire passenger manifest of a private company in exchange for payment. We believe the legal implications of such use should be further evaluated, as described in the Significant Concerns and Legal Implications section below.

Parcel Company Employees as Confidential Sources

The DEA established, utilized, and paid as Limited Use confidential sources, private parcel and courier company employees, as well as employees who work for

[23] The payment amount for this source is more than the amount identified in Table 7 for all sources reviewed because this amount reflects total payments as of January 2016, which is when we conducted our fieldwork. We found that between September 30, 2015, and January 11, 2016, this source was paid an additional $67,000.

mail reception companies.[24] During our review of confidential source files in two DEA Interdiction Units, we found that the DEA recruited these types of sources because they had access to company databases, access to parcels en route, or authority to administratively open parcels without a search warrant, which increases the potential for identifying suspicious parcels. We found that these confidential sources not only provided the DEA with information related to suspicious parcels, including parcel sender and recipient information, but at times also transferred customer packages to the DEA at the DEA's request. The DEA used information provided by these parcel company Limited Use confidential sources to perform background checks on the parcel recipients and, in some cases, to contact the associated customers or to conduct controlled deliveries of the packages in an attempt to develop a case. Successful parcel company-related consensual encounters and searches can result in the seizure of currency and illegal narcotics.

We performed an in-depth examination of five confidential source files associated with parcel industry employees. The DEA paid these Limited Use confidential sources more than $1.2 million during our period of review and more than approximately $1.6 million since their establishment. Table 8 gives an overview of the private parcel and courier company employee Limited Use confidential sources included in our review.

Table 8

FY 2011 to FY 2015
Nine Parcel Industry Employee Confidential Sources
Reviewed by the OIG

Confidential Source File Information Reviewed	Totals
Sources Tested	5
Number of Payments to Tested Sources	210
Amount Paid to Sources	$1,202,631
Cases	205
Total Currency Seized	$5,801,994
Number of Instances an Illegal Substance was Seized	1

Source: OIG analysis of DEA confidential source files

During our file reviews, we found that the DEA paid a parcel company employee confidential source, who was active for more than 12 years, over

[24] We attempted to analyze the DEA's CSSC data to identify confidential sources who were employed within the parcel and mail reception industry, but due to the numerous types and large number of different entities involved in this industry, as well as the inconsistencies related to the various methods DEA employees used to input employer information into CSSC, we could not estimate with any certainty the universe of DEA confidential sources employed within the industry. Therefore, our results for this industry are strictly based on the universe of parcel and mail reception industry confidential sources whose files we reviewed.

$1 million between FY 2011 and FY 2015 for contributions to 184 parcel interdiction seizures. As part of the confidential source's employment duties, the confidential source was allowed to administratively open packages that were in-process for delivery. When this confidential source administratively opened packages and found currency, the source would call the DEA to report it. The DEA would instruct this source to "over-box" the original package, address the new package to the Special Agent, and mail it to a different facility. Of note, we did not identify any drug-related cases or seizures associated with this confidential source and found that the confidential source only provided "tips" to the DEA for packages containing currency; we found no instances during our review period wherein this individual reported finding drugs or other contraband. We find this noteworthy, as it appears the DEA fostered a relationship with this source wherein the source provided packages that led to currency-only seizures, thus focusing the interdiction work toward cases that do not result in the prosecution of drug trafficking offenses. The DEA deactivated this source in April 2015, 5 months prior to our site visit, which according to a Special Agent was at the direction of DEA management due to scrutiny surrounding the use of these "professional" confidential sources. The same agent told us that the DEA's parcel interdiction work was negatively affected and almost eliminated by the deactivation of this parcel industry confidential source.

In a different office, we identified a confidential source who was a canine handler who appeared to provide services to a parcel company. Documentation in the file indicated that the source and his canine identified and notified the DEA of suspicious packages at the parcel company. After the DEA interdicted the packages reported by the confidential source, the DEA seized over $100,000. Consequently, the confidential source received an award payment of $19,600 for the "tip" that led to the seizure.

Significant Concerns and Legal Implications

We identified significant concerns and potential legal implications related to how the DEA field offices we tested used interdiction-related Limited Use confidential sources. These issues stemmed from the DEA's direction and guidance to the sources, long-term and lucrative relationships with these sources, and reliance on the sources to accomplish interdiction activities. Together, these factors call into question whether the source is truly providing information independently or is acting as DEA's agent, the latter of which could have implications relating to compliance with the Fourth Amendment's protections against unreasonable searches and seizures. In addition, these issues raise the question of whether these confidential sources fit the definition and spirit of a Limited Use confidential source.

During the OIG's prior investigations related to the DEA's use of Amtrak and TSA employees as confidential sources, the OIG found that the DEA's procedures did not provide for adequate DEA headquarters review over the establishment and use of these confidential sources. Based on both those investigations and this audit, we believe that the DEA's establishment, use, and payments to Amtrak and TSA employees were the consequence of insufficient oversight and weak controls

over the Confidential Source Program. These deficiencies are also persistent in the DEA's process for establishing, utilizing, and paying professional transportation and parcel industry employees as confidential sources in order to have access to private company information.

To obtain additional perspective, we discussed our concerns with the DEA's Chief Counsel's Office, an official within the Deputy Attorney General's office, and a Deputy Assistant Attorney General in the DOJ Criminal Division.[25] These officials told us that they could not provide an opinion on the appropriateness of these confidential sources because they had never reviewed or assessed the use of these confidential sources by the DEA for its interdiction program. Furthermore, the Deputy Assistant Attorney General stated that he was unaware of the frequency and large sum of payments to these confidential sources. The following sections provide specific information related to our concerns with the DEA's use of interdiction-related Limited Use confidential sources.

Direction to Limited Use Confidential Sources

As previously described, according to the DEA Special Agents Manual, the Limited Use confidential source is a professional business person who, independent of direction from the DEA, provides information to the DEA that could be independently corroborated by the DEA. The DEA compares its Limited Use confidential source category to what the AG Guidelines describe as a Source of Information. However, because the DEA travel and parcel industry confidential sources we have discussed here are generally utilized on a daily basis, for long periods of time, and with high compensation, we do not believe that these sources fit the definition of a Limited Use confidential source or Source of Information, as envisioned by the DEA Special Agents Manual or the AG Guidelines.

One of the foundational elements of the Limited Use confidential source relationship is that, while they may be recruited by the DEA, they must provide information "independently (without direction by DEA)." We found that some of the conduct we examined tested the boundaries of what it means to provide information without direction. We found that Special Agents asked sources with access to passenger travel databases to search for and provide the DEA with suspicious travel itineraries, as defined by the DEA, or for entire passenger manifests that contain manually entered markers to denote suspicious travelers. Further, Special Agents requested parcel employees to provide the DEA with information related to DEA-defined suspicious parcels and, at times, directed the

[25] The Deputy Assistant Attorney General for the Criminal Division we interviewed is the designated Department representative who participates on the DEA Sensitive Activity Review Committee (SARC). The SARC is responsible for performing the AG Guidelines-required review of long-term confidential sources and examining certain operational proposals to ensure the plans for proposed sensitive investigative activities are well founded and all issues of concern are sufficiently addressed. We discussed our concerns about activities related to DEA's Limited Use confidential sources with the DAAG because this official is knowledgeable of the DEA's Confidential Source Program and DOJ's narcotics-related law enforcement and prosecutorial activities.

employees to resend suspicious packages directly to the DEA. Moreover, during our review of confidential source files we noted instances wherein, subsequent to a seizure or in relation to other cases, Special Agents contacted these Limited Use confidential sources to obtain specific additional passenger information to further an investigation. In one of these instances, Special Agents requested a confidential source query private company systems and provide travel itinerary information for an airline passenger, and in another case the DEA requested the travel history for a passenger. In addition to appearing to constitute "direction," some of these DEA requests of confidential sources also are unlikely to align with the sources' legitimate and routine employer-assigned duties, and therefore present additional factors that conflict with the definition and spirit of a Limited Use confidential source. This practice also may not align, depending on the individual circumstances, with the AG Guidelines instruction that a law enforcement agency is never permitted to authorize a confidential source to participate in an act designed to obtain information for the agency that would be unlawful if conducted by a law enforcement agent.

When asked if the confidential sources informed their employers that they were working with the DEA, Special Agents stated that, similar to any confidential source, their work with the DEA should be confidential. Further, some Special Agents speculated that the employers would not condone the sources' relationships with the DEA and would likely terminate the confidential sources' employment if they knew of the relationships. Special Agents stated that the potential for termination is part of the inherent risk in cooperating and becoming a source for the DEA.

Based on our review of DEA policies and documentation, the Limited Use confidential source category coincides with confidential sources who provide "tips" to the DEA of pertinent facts passively observed during the course of routine duties related to employment. Yet we found that the relationship created by DEA Special Agents with some Limited Use confidential sources went beyond that of a professional person established as a confidential source who occasionally, and independently, provides "tips" related to suspicious activity observed during the course of their duties. Rather, certain of the confidential sources we reviewed appeared to be recruited and groomed to act on behalf of, or in partnership with, the DEA to continually provide pertinent, real-time information and at times take DEA-directed actions to advance investigations, all with an expectation of receiving potentially significant compensation.

Moreover, the long-term, lucrative relationship between the DEA and these travel and parcel industry employees, wherein the DEA recruits and requests that these Limited Use confidential sources perform inquiries on company systems or to provide information to the DEA about customer packages, and the emphasis on and necessity of these sources to the success of the DEA's interdiction efforts, further raises the question of whether these employees are truly acting independently, or acting as DEA's agents, the latter of which could have implications relating to compliance with the Fourth Amendment's protections against unreasonable searches and seizures.

Tracking and Handling of Confidential Source "Tips," and the Consequences for Subsequent Discovery Obligations

According to Special Agents from the field offices we visited, the DEA receives interdiction-related "tips" from Limited Use confidential sources so frequently that the Special Agents working interdiction efforts spend the majority, if not all, of their time acting on confidential source "tips." Further, these "tips" can be the primary basis for reasonable suspicion for stopping a passenger, requesting a consensual search, or intercepting a package to conduct a controlled delivery.

We identified significant concerns with how the DEA tracks the receipt of these tips. We found that Special Agents have various ways of receiving these "tips," but generally receive the information on a daily basis via email or text message, some of which are sent to government accounts and others to non-government private accounts that are established and controlled by the Special Agents. Additionally, we found that although some Special Agents estimated receiving up to 20 "tips," or passenger itineraries, per day from their Limited Use commercial airline confidential sources, the DEA does not maintain a record of receipt of the totality of the confidential source "tips." Rather, information about the tip is generally only maintained when there is a subsequent consensual encounter that leads to an arrest or seizure, and the retained information pertains only to the individual encounter.

The DEA requires that its confidential source files contain routine debriefing reports, applicable case initiation reports, and all contacts, events, or activity reports that document any activity of a confidential source. In addition, DEA policy requires that consensual searches be reported on a DEA-6 (Report of Investigation) investigative report within 5 working days of the search. However, during our review of the confidential source files, we did not find any documentation of any "tips" received from the confidential source unless there was a corresponding successful investigative activity, namely seizures of currency or drugs and arrests. Special Agents in the DEA field offices with Interdiction Units we reviewed informed us that the DEA does not keep track of the number of "tips" it receives from these Limited Use confidential sources or the total number of "tips" that DEA acts upon. Therefore, the files do not convey an accurate or complete view of the relationship between the confidential sources and the Special Agents. In addition, without tracking all of the confidential source "tips" and activities, we found that the DEA could not always provide detailed justification for payments to the confidential sources. Specifically, Special Agents told us that in order to keep sources motivated to continue providing "tips," they may pay sources for "tips" even if they do not result in arrests or seizures. As a result, in these instances the confidential source files may not contain documentation that connected those "motivational" confidential source payments to specific confidential source activity.

Because the DEA does not track or record this information, we could not, nor could the DEA, evaluate the totality of these confidential sources' contributions to DEA-related activities, to include how many "tips" the confidential sources provided

to the DEA, how often these "tips" resulted in consensual encounters, and whether those encounters led to searches and ultimately seizures or arrests. Moreover, the DEA is unable to examine whether the information DEA agents acted upon resulted in DEA mostly identifying individuals involved in illegal activity or instead caused them to regularly approach innocent civilians for questioning.[26] Consequently, the DEA does not have a full picture of all of the activity between DEA Special Agents and these confidential sources, which significantly diminishes the DEA's ability to oversee and manage the Confidential Source Program.

Further, we found that DEA Special Agents do not always include evidence that the investigation involved confidential source information in the applicable DEA-6 investigative report and do not always accurately cross-file the DEA-6 to the applicable confidential source file. Special Agents in one field office stated that they do not always mention the confidential sources' contributions because the DEA hopes to minimize exposure of the confidential source in the event that the DEA-6 must be provided for legal proceedings. One Special Agent also said that prosecution and defense lawyers know that this information is derived from confidential source "tips," so it is not necessary to explicitly explain this fact in the DEA-6. We believe that, in connection with DEA cases that lead to criminal charges, the failure to document all confidential source activity presents challenges to the tracking and retrieving of such activity, and therefore could increase the risk that some information relating to confidential sources may not be available to prosecutors when needed in connection with legal proceedings.

In addition, by receiving personally identifiable information on non-government private accounts, DEA Special Agents are risking that the information is not safeguarded with appropriate controls and, as a result, may be putting individuals' personally identifiable information (PII) at risk. Further, the use of non-government accounts has other implications. For example, such accounts may not be generally accessible by DEA in connection with required record searches, such as for legal processes and Freedom of Information Act inquiries. In addition, they may not be maintained in accordance with records retention regulations. We discussed this matter with DEA officials, who stated that they will continue to explore methods to improve DEA's operational security, vulnerability awareness and training, and evidence retention when interacting with confidential sources through electronic means.

---

[26] In the OIG's report on *The DEA's Use of Cold Consent Encounters at Mass Transportation Facilities*, January 2015, we found that the DEA did not collect sufficient data on cold consent encounters to enable it to assess whether the encounters were being conducted in an unbiased and effective manner. Our current audit revealed that DEA confidential sources are making significant contributions to DEA's interdiction activities, including providing tips leading to consensual encounters and searches. Because DEA's files did not provide sufficient detail on the universe of information provided by the sources, we similarly found that the DEA would be unable to determine if the confidential sources were applying unbiased or objective methodologies to their efforts to provide the DEA with information.

Extensive Reliance on Limited Use Confidential Sources

As described above, the DEA's interdiction activities are heavily reliant on the use of Limited Use confidential sources. While the DEA Interdiction Manual discusses the use of commercial airline and parcel company employees to obtain information for cases, the Interdiction Manual does not refer to these employees as confidential sources, nor does it contemplate that a paid relationship with these sources would or should be established. Nevertheless, we found that the DEA Interdiction Units we reviewed established many of these Limited Use confidential sources solely because the sources have access to private company databases and facilities, can provide DEA with "real-time" information pertinent to DEA's interdiction-related activities, and can also provide immediate responses for other investigative research. We confirmed this through a review of deactivation forms, which specifically indicated that the reason for deactivating many interdiction-related Limited Use confidential sources was that they no longer had access to an employer's passenger record system or package facility.

DEA Special Agents stated that these private companies would not otherwise provide the information to the DEA and that it could take months for a company to respond to an administrative subpoena request for the same information provided by the confidential sources. Moreover, these Special Agents also noted that the information provided by these Limited Use confidential sources could not be replicated or requested through any other process. Moreover, because it presumably takes time for confidential sources to learn how to identify suspicious itineraries and packages, Special Agents told us that when they find a source who is proficient with the process, they strive to keep them active through monetary incentives. These considerations, combined with the importance of these Limited Use confidential sources to the DEA's interdiction efforts, provided strong incentives for the DEA field offices in our review to create a system that encourages these sources to develop lucrative long-term relationships with the DEA.

The full extent to which these relationships can be lucrative to a confidential source is best illustrated by examining the 4 confidential sources who worked for a commercial airline, Amtrak, a private bus company, and a parcel company, respectively, and were paid an average of more than $100,000 per year between FY 2011 and FY 2015. The following table provides an overview of the payments made to these four individuals, who were the highest paid Limited Use confidential sources within our sample from each industry discussed in our report.

Table 9

FY 2011 to FY 2015
Highest Paid Limited Use Confidential Sources Reviewed by Type

Confidential Sources	No. of Payments FYs 11-15	Amount Paid FYs 11-15	Total Years Active	Total Paid Historically
Amtrak Employee	74	$726,439	18½	$962,615
Commercial Airline Employee	133	$617,676	3[a]	$655,744
Bus Company Employee	78	$362,112	4[a]	$429,212
Parcel Industry Employee	186	$1,042,117	14	$1,430,292

[a] These confidential sources were active and receiving payments at the time of audit testing. The total years active was calculated based on the date of audit testing.

Source: OIG analysis of DEA confidential source files and CSSC data

The frequency of payments to these confidential sources and the large dollar amounts involved underscore the importance of properly classifying sources, properly overseeing the payments made to them, and fully understanding the extent to which these individuals are used and relied upon. Yet we determined that, because these sources have been categorized as Limited Use and the types of interdiction cases they contribute to are generally resolved through non-criminal forfeitures, or are, as DEA Special Agents generally described them, "open and shut cases," there is minimal internal oversight of the DEA's extensive use of these Limited Use confidential sources. As mentioned, representatives from the DEA's Chief Counsel's office stated that they have not reviewed the propriety of this type of activity. We believe that the deficiencies we identified in the DEA's use, handling, and compensation of Limited Use confidential sources discussed in this report raise serious questions about the appropriateness of these activities.

THE DEA INTELLIGENCE DIVISION'S OVERSIGHT OF CONFIDENTIAL SOURCE ACTIVITIES AND THE DEA'S USE OF SUB-SOURCES

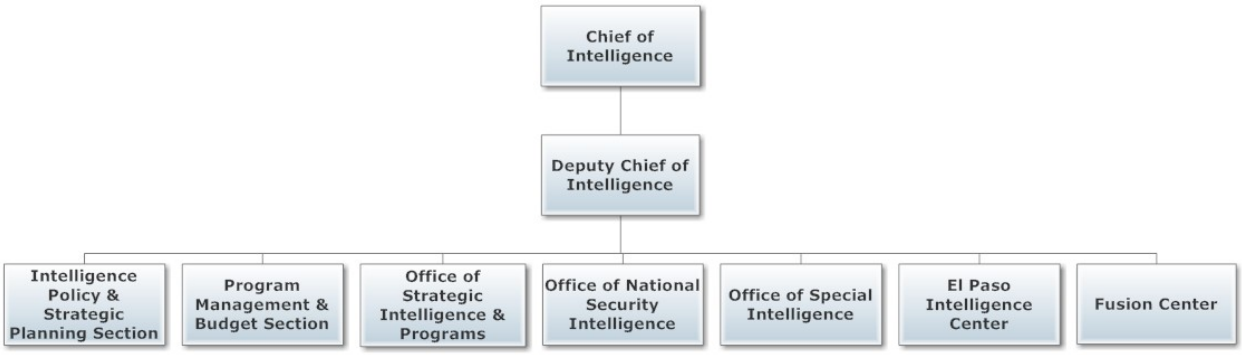
The DEA's Intelligence Division paid approximately $30 million to confidential sources between FYs 2011 and 2015 to provide narcotics-related intelligence and assist in law enforcement operations. We found significant weaknesses in the DEA's management, oversight, and accountability of intelligence-related confidential source information, activities, and payments. In addition, we found that some DEA confidential sources, including some used in intelligence-related work, employed "sub-sources" and that this practice was condoned by the DEA. Because the DEA has not established processes or procedures to manage the use of "sub-sources," such as a risk assessment or other oversight and control mechanisms, we believe that the use of "sub-sources" pose significant risks to the DEA and should be further evaluated.

DEA Intelligence Division's Confidential Source Payments and Utilization

The DEA's Intelligence Division collects and produces narcotics intelligence through a variety of operations, programs, and initiatives. There are seven primary sections that comprise the Intelligence Division, as identified in the following figure.

Figure 1

Intelligence Division Organizational Chart



Source: DEA

These DEA's Intelligence Division sections coordinate with the DEA operational offices to initiate new investigations and enhance ongoing investigations and prosecutions. In addition, the DEA's Intelligence Division works with outside agencies that produce or use narcotics intelligence to increase the efficiency in the reporting, analysis, storage, retrieval, and exchange of narcotics-related intelligence information within the U.S. Government. The DEA's Office of National Security Intelligence, which falls under the DEA's Intelligence Division, is a member

of the Intelligence Community, and through this Office the DEA coordinates the provision and receipt of drug-related national security information with other members of the Intelligence Community.

During our audit, we found that the majority of offices within the DEA's Intelligence Division do not establish confidential sources or directly work with sources, but rather provide funding to domestic or international field offices, including the Special Operations Division, to pay for confidential source-related activities associated with the collection of information or provision of services for intelligence programs. We reviewed documentation related to six Intelligence Division programs for which the DEA paid confidential sources for information and services.[27] In general, these intelligence-related programs focus on obtaining insight into operational activities of drug trafficking organizations. In addition, these programs attempt to identify drug trafficking-related intelligence gaps, risks, and threats in field offices' areas of operation, as well as to predict the amount of drugs produced in certain parts of the world.

We also reviewed 10 confidential source files associated with sources who were used by the Intelligence Division. Based on our review of documentation and confidential source data, we estimate that the DEA's Intelligence Division paid approximately $30 million to confidential sources between FYs 2011 and 2015. Overall, we found that the Intelligence Divisions' tracking process and oversight did not adequately account for payments to confidential sources or the services and information provided by these sources that would justify payments. As a result, the DEA's Intelligence Division is not ensuring that the funding it spends on these payments are advancing DEA's intelligence-related programs, as described in the following sections. Further, for all but one program, the Intelligence Division has relied on a decentralized approach for ensuring that the confidential sources who provide drug-trafficking related intelligence are properly vetted and managed, and this approach does not provide for adequate oversight and review.

Confidential Source Validation

Intelligence Community entities often utilize human sources of information to assist in accomplishing their missions. As previously noted, the DEA's Office of National Security Intelligence is a member of the Intelligence Community and, although this Office has not specifically established or controlled any confidential sources, it often includes confidential source information in its intelligence products. The Office of the Director of National Intelligence has promulgated standards for the appropriate handling of these individuals, including validation of the sources and

[27] Throughout this audit finding, we do not provide specific details about the DEA Intelligence Division's operations, programs, and confidential sources because of the sensitivity and classification of the subject matter. Some of the DEA's activities in this realm are controlled through restricted access limitations, which the DEA developed in consultation with the Department. The DEA exercises these controls by limiting access to individuals who have been briefed by the DEA on certain classified programs on which the DEA works. Therefore, we will separately provide more detailed information on our audit results specific to these areas to authorized individuals with an appropriate clearance.

the information they provide. In comparison, the DEA currently does not implement an independent validation or review process for its confidential sources because, according to DEA officials, all of its confidential sources are used primarily for law enforcement purposes, not solely for national security or Intelligence Community work. DEA officials told us that further validation of information or of the confidential sources could result in delays to act on or provide the information to its Intelligence Community partners, which could reduce the value of the information. In addition, DEA legal and intelligence officials expressed concern over applying the Intelligence Community's validation and rating process to the DEA's confidential sources because they believe this would impact the ability of prosecutors to effectively utilize DEA confidential sources during narcotics-related criminal proceedings.

However, the DEA's Intelligence Division uses information obtained from confidential sources for its narcotics intelligence-gathering programs. In FY 2013, the DEA transferred Special Agents to one of its Intelligence Division offices so that it could establish, utilize, and pay its own confidential sources in connection with one of its programs.[28] According to DEA officials associated with this program, the DEA also instituted a multi-faceted review process to assess the validity and utility of the information provided by these confidential sources, which we believe, based the officials' description, could be a very lengthy process.

Although the DEA, for the above-referenced program, has begun some information validation and reliability assessments, the DEA has not implemented a reliable and responsive process for all of its intelligence-gathering programs. According to officials associated with other Intelligence Division programs, those programs have not instituted processes for ensuring the validity and reliability of information provided by confidential sources. These Intelligence Division programs are thus relying upon the field offices' determination that the information is accurate and the confidential sources are reliable. As a result, the Intelligence Division has not implemented a consistent process to ensure the integrity of confidential sources and of their information that DEA uses for its intelligence-gathering programs.

In contrast to the DEA, the Federal Bureau of Investigation (FBI), DOJ's other Intelligence Community member, has implemented an independent validation process that applies to its confidential human sources, including those used for intelligence purposes, for law enforcement efforts, or both. This independent and centralized process requires the FBI to assess the reliability, authenticity, integrity, and overall value of a given source based on various risk factors. According to the FBI, the validation process requires a periodic independent FBI headquarters review of sources, including an evaluation of sources in a broad, national context. We believe that the DEA would benefit from discussing with the FBI its procedures for

[28] The DEA Special Agents Manual requires that confidential sources be handled by Special Agents. Employees in other types of positions, such as Intelligence Analysts, are prohibited from handling confidential sources. Prior to FY 2013, the referenced office did not have any Special Agent positions.

independently assessing sources and the impacts of this process both on the timeliness of information sharing and on subsequent criminal prosecutions, with the goal of implementing an independent review process that better ensures the reliability and accuracy of confidential source information, and better reflects the standards employed at other Intelligence Community entities. Additional oversight by the Intelligence Division is particularly important given the deficiencies in field office oversight of confidential sources, as described throughout this report and in our 2015 report.

Intelligence Division Oversight of Confidential Source Payments

According to Intelligence Division officials, Intelligence Division funds provided to field offices generally are used to pay confidential sources to provide intelligence-related information to the DEA, which may entail also having to pay for a sources' travel expenses associated with intelligence-gathering endeavors or for sources to participate in drug buys. For confidential source payments, DEA Intelligence Division officials told us that the process to request funding generally requires field offices to provide an email to the Intelligence Division that describes how a confidential source can address an intelligence gap and references a case number associated with the confidential source's information and services. Once Intelligence Division officials approve the request, the funds are transferred to the field office, and the Intelligence Division presumes that the funds are used as described. However, according to Intelligence Division officials the Intelligence Division does not follow up with field offices to determine if the desired information or service was actually provided, or whether the information adequately satisfied the intelligence gap.

We asked DEA Intelligence Division officials to provide us with an overall total, and an itemized list, of payments associated with intelligence-related confidential sources during our review period of FY 2011 through FY 2015. The Intelligence Division was unable to do so because it did not aggregate this information and, although the Intelligence Division keeps a tracking log for fund transfers to field offices for some of its intelligence-related programs, it did not always track these payments to the level of detail that would allow them to discern confidential source-related payments in particular. Officials instead provided us with the overall tracking log, which we found did not always include payment information by field office, confidential source number, or investigative case file. We also found that not all of the programs employing confidential sources were included in the log. However, based on our review of this log, we concluded that the Intelligence Division spent approximately $1 million each year between FY 2011 and FY 2015 on payments to field offices for 5 intelligence-related programs, which included (but was not limited to) payments to confidential sources.

In addition, we identified at least nine confidential sources who were specifically associated with another intelligence program run by the DEA's Intelligence Division during our review period. Of those 9 confidential sources, we found that according to CSSC the DEA paid 8 individuals approximately $25 million between FYs 2011 and 2015. However, the DEA did not keep records of all of the

confidential sources paid for information and services related to intelligence programs, so we cannot definitively determine how many sources or how much money the DEA paid sources for this program in total.

Through our file reviews, we identified that the DEA paid one of these confidential sources whom the DEA categorized as Protected Name more than $30 million over a 30-year period. We found that the DEA's Intelligence Division would transfer funds through a wire transfer to the field office that established the source for Special Agents to pay the confidential source. This is divergent from the DEA's standard process of utilizing a field offices' Imprest Fund account to obtain cash for confidential source payments because the payment amounts were so large – more than $400,000 in certain instances – the cash was not available through the Imprest Fund account.[29] We found that the non-standard process used to pay this source resulted in the improper tracking of $2.7 million in payments to this source between FYs 2011 and 2013, and that not all payments to the source were recorded in the DEA's electronic confidential source system, CSSC. DEA officials told us that they stopped this practice.

As described, in FY 2013 the DEA's Intelligence Division began controlling and paying some confidential sources associated with this program directly rather than relying on assistance from domestic field offices. DEA officials believe that this is a marked improvement from the previous process established by the Intelligence Division for this program. However, the oversight employed by the DEA's Intelligence Division still is not commensurate with the significant amount of money that it pays to confidential sources. Specifically, of the nine sources that we reviewed, DEA initially categorized eight of them as Limited Use or Regular Use. While the DEA eventually revised that categorization to Protected Name, for five of these sources the Intelligence Division received an exception from DEA's Chief of Operations Management that allowed the DEA to follow the oversight and review requirements of a Limited Use confidential source.[30] According to Intelligence Division officials, they requested this exception because the requirements associated with the Protected Name source category would have caused security concerns for the sources, and would have required the handling Special Agents to travel excessively to accomplish quarterly debriefings. Yet this exception also resulted in the DEA exercising less oversight of these highly-compensated sources, and requiring a lower level of supervisory approval and assessment for their establishment, use, and overall management.

The DEA's Use of Sub-sources in Enforcement and Intelligence Activities

During our review of confidential source files at DEA field offices and the Intelligence Division, we found that some confidential sources enlisted the

[29] Imprest funds are fixed or petty-cash funds held in the form of currency and coins outside the Department of Treasury that are advanced to designated cashiers, who in turn advance the funds to employees for mission-related expenses.

[30] Table 2 provides the requirements related to the different confidential source categories.

assistance of additional individuals to acquire information or to perform services for both DEA law enforcement investigations and intelligence programs. The DEA generally refers to these individuals, who have no formal or direct association with the DEA, as "sub-sources." Our review found some sources received a substantial amount of compensation from the DEA and the file indicates that the source was expected to provide some of those funds to sub-sources. In some instances we reviewed, the DEA explicitly agreed to pay confidential sources for information provided or work conducted by "sub-sources." However, it was not always clear from the documentation whether the confidential source had informed the "sub-source(s)" of their relationship with the DEA, or whether the DEA knew the identity of or amounts paid to the "sub-source(s)."

We found that although DEA officials were aware of this "sub-sourcing" practice by some of its confidential sources, the DEA had not established processes or procedures to govern the risks inherent in paying for and using information provided by a "sub-source." These risks are substantial. For example, if the DEA cannot identify the individual who is providing information or services, it cannot perform assessments to ensure that the individual is reliable, trustworthy, and not an adversary. The use of "sub-sources" to provide services and information intended to assist the DEA without the DEA's full knowledge and awareness also increases the chance that individuals may be conducting unauthorized illegal activity on the DEA's behalf.

In 2005, the OIG identified the DEA's use of sub-sources as a concern and noted in the report that the OIG observed 17 payments totaling $52,240 specifically made to sources for sub-sources. At the time, the OIG did not make a recommendation related to the DEA's use of sub-sources, but alerted the DEA to the matter. However, our identification of this continued practice and the lack of guidance for the use or prohibition of "sub-sources" indicates that the DEA has not adequately evaluated this area of the Confidential Source Program. Furthermore, we believe that the DEA has not fully considered all of the significant risks involved with condoning the use of "sub-source(s)."

DEA CONFIDENTIAL SOURCE OVERSIGHT AND MANAGEMENT

DEA Confidential Source Program oversight and management are carried out by both DEA field office and headquarters personnel. We identified numerous deficiencies with the DEA's oversight and management of confidential sources, some of which were previously identified in the OIG's 2005 audit report. We found that the headquarters-based Confidential Source Unit relies too heavily on the judgment of field office personnel for many aspects of its Confidential Source Program and has not provided adequate oversight to ensure that decisions related to confidential source establishment, use, and payments are appropriate. In addition, the DEA does not perform comprehensive reviews of the field offices' activities related to confidential sources, and what oversight the DEA does perform has been inconsistent and inadequate. As a result, we noted substantial variations in how confidential sources are categorized, as well as concerning instances wherein confidential sources were deactivated due to unsatisfactory behavior yet continued to receive payment after deactivation. In addition, we found that the DEA did not adequately review or ensure that the information in its electronic data system concerning confidential sources was complete, consistent, and accurate. Finally, based on the significant deficiencies we identified related to the DEA's tracking, justification, and documentation of payments to confidential sources, we concluded that the DEA did not institute sufficiently strong internal controls over confidential source payments. Given the sensitivity and importance of this program, we believe there is a vital need for enhanced oversight to mitigate the risks we have identified.

In our July 2015 audit report, we identified various instances where the DEA's Confidential Source Unit did not adequately coordinate with other DEA entities involved in confidential source-related activities.[31] The lack of coordination caused problems for the DEA in terms of implementation, oversight, and compliance with certain policies and procedures. Throughout our continued audit work, we concentrated on the risks associated with DEA Limited Use and intelligence-related confidential sources. Nevertheless, in conducting our audit we identified numerous deficiencies with the DEA's oversight and management of confidential sources more generally, some of which were previously identified in the OIG's 2005 audit report of the DEA's payments to confidential sources.[32] These deficiencies, which indicate a need for more proactive and coordinated headquarters oversight and monitoring of the Confidential Source Program, are described below in further detail.

---

[31] OIG, *Audit of the DEA's Confidential Source Policies and Oversight of Higher-Risk Confidential Sources*, Audit Report 15-28 (July 2015).

[32] OIG, *The DEA's Payments to Confidential Sources*, Audit Report 05-25 (May 2005).

Confidential Source Program Oversight Responsibilities

The DEA's processes for confidential source oversight, management, and review are generally implemented by field office Special Agents and management officials, the Confidential Source Unit, and the Inspections Division.

The field offices have the primary responsibility for assessing, establishing, using, and paying confidential sources. Special Agents debrief sources, perform risk assessments, and complete administrative forms to activate and deactivate confidential sources. Depending on the categorization of a confidential source, the establishment of a source must be approved at the field office level by either the Group Supervisor, an Assistant Special Agent in Charge, or the Special Agent in Charge. The personnel in these positions also determine and approve the justification and amount for confidential source payments. Additionally, at each field division, a Confidential Source Coordinator is assigned to maintain the confidential source file and to serve as liaison between the field offices and the Confidential Source Unit in DEA headquarters. Based on interviews with personnel from the 9 field offices we visited, we found that many Special Agents and Supervisory Special Agents often identified their initial training as a Special Agent, but stated that they rely upon "on-the-job" training and the advice of their peers regarding establishing, approving, utilizing, and paying confidential sources. In addition, Confidential Source Coordinators we interviewed stated that they do not validate or perform a comprehensive review of confidential sources and generally provide only administrative support to Special Agents and Supervisory Special Agents.

The DEA's Confidential Source Unit is the primary DEA headquarters entity responsible for managing the Confidential Source Program for the DEA. The unit's responsibilities include approving establishment and continued suitability forms, assigning confidential source numbers, approving requests that require senior official approval, providing guidance to Confidential Source Coordinators, and managing aspects of CSSC. An official from this Unit referred to the Unit as the field's "customer service" office for confidential source-related matters, while another official from this Unit stated that they generally accept field offices' confidential source decisions and approvals.

The DEA's Inspections Division's processes are one of the main sources of confidential source review. Generally, the Inspections Division conducts on-site field office inspections every 4-5 years. Inspections include a review of confidential source files and require inspectors to conduct interviews with at least 50 percent of active confidential sources. In addition, the Inspections Division requires field offices to conduct annual self-inspections, which also entail confidential source file reviews and interviews. According to DEA officials, the Inspections Division's review is a "check" to ensure that the field offices are appropriately self-reporting issues related to the Confidential Source Program. Based on our assessment of the office inspection process for confidential source matters, we found that it generally focuses on compliance and does not incorporate a substantive review of confidential source establishment, utilization, and payment. This finding is consistent with the

statement of an Inspections Division official, who told us that the purpose of the Inspections process, as it relates to confidential sources, is to ensure that proper documentation is available in the field for field office managers to assess the utilization of sources; the inspections process does not assess confidential source establishment and utilization decisions, or justification for payments. We also found that the Inspections Division reports do not include a summary assessment of the totality of all compliance issues found or any overarching areas of improvement needed in a field office's Confidential Source Program.

In light of the deficiencies we identified during this audit, including the DEA's use of Limited Source confidential sources, the Intelligence Division's substantial payments to confidential sources, the lack of guidance concerning the use of "sub-sources," and other deficiencies described below, we believe that the Confidential Source Unit and Inspections Division, as the primary offices with oversight and management responsibilities, should execute more robust oversight methods to review field offices' establishment, use, and payments to confidential sources. These offices are unique within the DEA for their broad perspectives on the Confidential Source Program, and we believe they should use that perspective to ensure that the field offices' decisions related to confidential sources are consistent, appropriate, and thorough.

Confidential Source Categorization and Use Inconsistencies

The confidential source establishment process, which generally includes a risk assessment, happens primarily at the field office level. Appropriate categorization of sources is imperative to ensure adequate oversight and compliance with both DEA and AG Guidelines directives for certain sources. In addition, we believe that a consistent and accurate process for source categorization is necessary for a well-functioning and effective Confidential Source Program. During our confidential source file reviews, we identified the following concerns regarding inconsistencies in the decision process for confidential source categorization.

Application of Confidential Source Category Based on Criminal History

The DEA Special Agents Manual stipulates that Special Agents must check the National Crime Information Center (NCIC) database for criminal histories, warrants, and recent arrests.[33] However, the DEA Special Agents Manual does not provide clear and consistent guidance to Special Agents for how a confidential source's criminal history affects the categorization of the source. Specifically, the DEA Special Agents Manual allows for the use and payment of confidential sources with criminal histories under the category of Restricted Use. (See Table 2 for the requirements associated with the various categories of confidential sources.) For the Restricted Use confidential source category, the DEA requires a greater degree

[33] NCIC is an electronic clearinghouse of crime data, managed by the FBI that can be accessed by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year to obtain criminal history information.

of supervisory control and specifically cites the need for additional oversight if the confidential source has previous offenses involving acts of violence against persons, felony sex offenses, felony or misdemeanor offenses involving dishonesty or false statements, or perjury. Although the Restricted Use category is the only category that references the existence of a criminal history, other categories, such as Regular Use and Defendant, contemplate the lack or existence of a criminal history through the category definition. However, the DEA Special Agents Manual does not specifically prohibit confidential sources with criminal histories from being categorized as Limited Use. Rather, this section of the DEA Special Agents Manual only states that to meet the categorization criteria for Limited Use, the confidential source must not provide information that is the result of any type of criminal association. We also determined that DEA policy does not preclude a single source from being simultaneously placed into different categories by different DEA field offices, a practice that would increase the risk of inconsistent and potentially improper direction and supervision.

During our review of confidential source files, we identified instances where the Limited Use category was used inconsistently for confidential sources with criminal histories. Specifically, at two field offices we visited, we identified Limited Use confidential sources whose criminal history reports included arrests for providing false information to law enforcement, allegations of drug trafficking, and battery. Special Agents and managers from these field offices stated that according to their interpretation of the DEA Special Agents Manual, criminal history does not exclude a person from being established as a Limited Use confidential source. These DEA officials also told us that for these Limited Use confidential sources, the individuals' criminal histories did not affect their ability to provide services or informational "tips" to the DEA, a statement that we found implausible for at least some of the criminal histories we reviewed. For example, using for interdiction activities a Limited Use confidential source who was arrested previously for providing false information to law enforcement significantly increases the risk that the source is unreliable and therefore that person should be subject to more oversight than normally afforded to those in the Limited Use category.

In contrast, we found that a different field office established a "tipster," who was a parcel employee with a criminal history record and used in an Interdiction Unit, as a Restricted Use confidential source rather than a Limited Use confidential source. According to a Special Agent from that field office, the individual did not qualify as a Limited Use confidential source due to the criminal history and instead had to be established as a different category of source to be in compliance with the DEA Special Agents Manual. Thus, in handling the source, this field office followed the enhanced supervision requirements associated with Restricted Use sources, as displayed in Table 2.

We believe that the absence of definitive policy regarding this aspect of confidential source management increases the risk that inappropriate individuals will be established as confidential sources or that sources will not be adequately handled and supervised. As such, we believe that the DEA should reevaluate its policy to ensure that it establishes appropriate procedures and controls for

confidential sources with criminal histories, and for ensuring that concurrent use sources are categorized, used, and supervised appropriately.

Payments to Deactivated Confidential Sources

The DEA Special Agents Manual stipulates that Special Agents may not pay any deactivated confidential source who was deactivated due to the source being the subject of an arrest warrant or who committed any serious offenses. During our review, we found two instances of payments to previously-deactivated sources that, under the circumstances, raise serious questions of propriety.

In the first instance, the DEA reactivated a confidential source who was deactivated for unsatisfactory behavior or performance because the source had previously provided false testimony in trials and depositions.[34] This reactivation was approved by DOJ officials, as well as executive-level DEA officials. During the period of reactivation, which lasted approximately 5 years, we found that 13 DEA field offices used this "unsatisfactory" confidential source, categorized the source as Restricted Use, and paid the source more than $400,000. According to documents in the confidential source's file in one DEA field office, the confidential source provided false statements to a prosecutor during the course of an investigation and engaged in behavior that created adverse publicity for the DEA. The DEA field office involved in that particular investigation deactivated the confidential source for unsatisfactory behavior on June 24, 2013 – the second time this source had been designated "unsatisfactory."

DEA policy states that any confidential source declared "unsatisfactory" in an investigation generally would not be considered for award payments or monetary compensation. However, based on our review of CSSC data, we concluded that both the deactivating field office and another concurrent use field office continued to pay the confidential source after the second "unsatisfactory" designation. Specifically, according to CSSC, between June 24, 2013, and October 24, 2014, the DEA paid this confidential source more than $61,000 in both award payments and payments for information – increasing the total amount paid to this source to $469,158.

In the second instance, we found that on July 31, 2014, the DEA deactivated a Limited Use confidential source who was the subject of an ongoing OIG investigation. The OIG reported that as of January 2014, the DEA inappropriately paid the confidential source, who was an Amtrak employee, over $850,000 for

[34] The DEA Special Agents Manual identifies procedures to deactivate a confidential source for unsatisfactory behavior or performance. Situations that warrant such an unsatisfactory deactivation include a confidential source providing false statements; committing perjury; committing a felony offense; failing to obey DEA instructions; absconding with DEA funds, equipment, or controlled substances; withholding or planting drug or nondrug evidence; compromising an investigation; failing to appear for trial or pretrial conferences; or engaging in behavior that is likely to endanger DEA or other law enforcement personnel or operations, pose a threat to public safety, or create adverse publicity for DEA. Declaring a confidential source unsatisfactory prohibits the use of the source by any DEA office, unless formally re-established pursuant to heightened levels of approval and notification.

information that was available at no cost to the government, thereby wasting substantial government funds.[35] However, according to CSSC and our review of this confidential source's files, the DEA paid this confidential source a total of $962,615, of which more than $44,000 in award payments was paid after deactivation.

While DEA policy allows deactivated confidential sources to receive payments that are already in process, we believe that in these instances the payments to the previously-deactivated confidential sources were not warranted because of the issues surrounding the sources' deactivation. In the first case, the source committed wrongful acts that negatively impacted the DEA and twice resulted in his being labeled "unsatisfactory." In the second instance, the DEA scrutinized the overall use of these confidential sources and deemed their use ill-advised, which not only makes payments to these confidential sources during activation questionable, but also challenges the DEA's reasoning for post-deactivation payments to these sources, which only added to the waste of taxpayer funds. In these instances, we believe that the DEA officials who requested and approved the payments did not thoroughly assess the justification for payments and, thus, unnecessarily wasted government funds.

In addition, based on our analysis of the DEA's CSSC data, we estimated that the DEA paid approximately $9.4 million to more than 800 deactivated confidential sources between FYs 2011 and 2015. While we describe in this report some concerns about the accuracy and completeness of the data available from the DEA, and we did not review the circumstances of all of these payments, it appears from the information available that paying deactivated sources is common enough at the DEA to justify much closer managerial oversight and review of such payments.

Confidential Source System Concorde Use and System Deficiencies

The DEA uses CSSC to manage and record payments to confidential sources. While CSSC is not the official system of record for confidential source information, it retains electronic information related to the utilization of confidential sources. It also contains payment information that is either ingested in daily feeds from the Unified Financial Management System (UFMS) or is manually entered by DEA personnel.[36] For security reasons, the DEA restricts access to CSSC information to select personnel. In the field, only the Confidential Source Coordinator, controlling Special Agents, and their supervisors have routine access to CSSC and the official confidential source files. Within DEA headquarters, CSSC access is generally restricted to personnel from the Confidential Source Unit and the Office of Information Systems.

---

[35] OIG, *DEA's Use of Amtrak Employees*.

[36] The United Financial Management System is an integrated solution that provides electronic financial transaction processing across numerous DOJ components. The DEA uses UFMS for financial management and this system contains transaction-level information for the DEA's payments to confidential sources.

During FY 2011, the DEA implemented CSSC as a system that assists in the management of confidential sources. The development and implementation of CSSC was, in part, responsive to OIG recommendations in our 2005 confidential source audit report, prior to which the DEA had an inadequate method of source data management. During this audit, we found that the DEA has not fully deployed all aspects of CSSC to successfully capture pertinent confidential source information that can enhance the DEA's oversight of the Confidential Source Program. In addition, the control settings within CSSC are insufficient to ensure that information entered into the system is captured in a complete, consistent, and accurate way.

For instance, CSSC includes fields regarding a confidential source's employer, skills, and occupation, which we believe are imperative pieces of information for the DEA's risk assessment, categorization, approval, use, and oversight of confidential sources. In fact, the AG Guidelines and the DEA Special Agents Manual identify specific occupations and employers that require additional scrutiny, and in some cases high-level approval. However, during our review of CSSC data, we found instances where these data fields were not used consistently, not verified, or sometimes not completed.

We also found weak system controls in CSSC. For example, DEA Special Agents are able to bypass certain mandatory fields because the system settings do not identify them as mandatory. Additionally, lack of clear guidance on what information is required and where certain information should be annotated, as well as inadequate review of the information entered into the system, has resulted in inconsistencies in CSSC data and the loss of valuable information. In addition, the Confidential Source unit does not ensure that fields have a valid value entered and has not conducted a validation review or statistical analysis of confidential source data in CSSC. Such a review could have identified the inconsistencies and incomplete data fields we found during our review.[37]

We believe the inaccuracy and incompleteness of this data reduces the value of CSSC in at least three ways. First, it inhibits the DEA's ability to monitor confidential source activity and to identify confidential sources who have certain skill sets or associations that are needed for DEA operations or oversight. For example, as mentioned in the section entitled Limited Use Confidential Source Involvement in DEA Interdiction Activities, DEA headquarters officials were unaware that field offices continued to establish and utilize Amtrak employees as confidential sources after the OIG issued investigative reports addressing these practices. We believe that improved internal controls over the accuracy and completeness of information entered into CSSC could have allowed the DEA to more readily determine and track the number of Amtrak and TSA-related confidential sources for headquarters review and oversight.

---

[37] For example, during our review of Limited Use confidential sources used in interdiction activities, we attempted to identify sources by employer and occupation using various data fields. Through basic data queries, we found that 6 percent of Limited Use confidential sources did not have such information recorded in CSSC. Such a query would have been easy for the DEA to replicate.

Second, inaccurate and incomplete data can inhibit the DEA's strategic and proactive use of CSSC to manage and oversee the Confidential Source Program. Although DEA officials within the Confidential Source Unit told us that they do not currently use CSSC as an oversight tool to identify strengths, weaknesses, and trends, nor as a means to more strategically manage the Confidential Source Program, we believe that such uses will become increasingly beneficial as controls are improved and the data becomes more reliable and complete.

Third, DEA officials stated that they may use information from CSSC or directly from confidential source files to comply with discovery obligations during criminal proceedings. Thus, it is imperative that CSSC and confidential source file information is accurate, consistent, and complete.

Payment Oversight and Management

Based on our analysis of the DEA's CSSC data, we found that between FY 2011 and FY 2015, the DEA paid approximately $237 million to its domestically established confidential sources. During our review of confidential source files, we found deficiencies in the DEA's tracking and oversight of payments to confidential sources, as described below.

Payment Tracking Discrepancies

We examined 120 confidential source files and compared the payment information to that within the CSSC data we analyzed. We also completed a limited reliability check of CSSC data, which is discussed in the Objective, Scope, and Methodology appendix to this report. We found numerous exceptions, including those listed below:

- Payments missing from CSSC – We found documentation in a confidential source file that supported payments to a confidential source totaling approximately $3 million, but CSSC did not reflect these payments. We asked DEA officials about these missing records and were told that these payments did not appear in CSSC because they were mistakenly identified as payments to the Special Agent who requested the payments to the confidential source. Based on this discrepancy, a DEA finance official queried UFMS and found more than $650,000 in additional confidential source payments that were incorrectly associated with Special Agents rather than confidential sources. This DEA official corrected these payment entries in UFMS to associate them to the confidential source who received the payments.
- Duplicate payment entries in CSSC – During our testing of three confidential sources, we identified numerous instances where the CSSC record indicated payments that were not supported by hard-copy documents in the source file. In analyzing these payments, we found that they appeared to duplicate other payments because they included the same amount and case number.

We informed DEA officials of this issue, and after reviewing CSSC and UFMS, they confirmed that the entries were duplicates, but that the sources had only been paid once. The DEA officials believed that this was possibly the result of payments being entered twice, once into UFMS by finance personnel and a second time into CSSC by a Confidential Source Coordinator.

- Incorrect payment reason type in CSSC - We found instances wherein confidential source payment reasons entered into UFMS included transaction categories for which confidential sources should not be compensated, such as a lease or extended temporary duty. We inquired with a DEA official to determine why these payment categories were used for confidential source payments. According to the official, these are examples where an incorrect payment reason type was input when the payment was entered into UFMS. As CSSC imports confidential source payment information directly from UFMS, the information related to these payments was also incorrect in CSSC.

These missing payments, duplicate payment entries, and incorrect payment reasons appear to be widespread and negatively impact the accuracy of the payment information contained within CSSC, and therefore the usefulness of CSSC itself. Although the physical confidential source file containing confidential source paperwork is the official file, CSSC allows Special Agents and Confidential Source Coordinators to track and monitor annual and lifetime payments. The accuracy of the information is therefore imperative to ensure compliance with the DEA Special Agents Manual and AG Guidelines requirement for additional levels of approval for many confidential sources who receive more than $100,000 annually and $200,000 in a lifetime.[38] In addition, we found that some of the DEA Confidential Source Coordinators we interviewed use CSSC data to report payment information during the discovery phase of a criminal prosecution. Thus, the accuracy of the CSSC payment information is not only essential to DEA's management of the Confidential Source Program, but also to ensure that the government satisfies its discovery obligations during a criminal proceeding.

When we discussed this issue with DEA officials in the Inspections Division, the Confidential Source Unit, and field offices, they all agreed that developing a process to reconcile payment information within CSSC and confidential source files was a good idea. Inspections Division officials stated that this procedure could be incorporated into the inspections process. Therefore, we recommend that the DEA develop a process to reconcile payment information in CSSC with documentation in the confidential source file to ensure consistency, completeness, and accuracy of confidential source payment information.

[38] This audit did not attempt to conduct a full assessment of how the DEA implements this requirement. However, the evidence we reviewed suggested that the requirement does not trigger additional levels of approval for some highly paid DEA confidential sources, either because of how the confidential sources are classified or because the form of some payments to these sources are not counted towards the annual or lifetime amounts.

Payment Support and Documentation Discrepancies

To begin processing payments to confidential sources, Special Agents are required to submit to fiscal personnel both a DEA-12 form (Receipts for Cash or Other Items) and a DEA-103 form (Voucher for Purchase of Evidence or Payment to Confidential Source). In addition, award payments to confidential sources from the Assets Forfeiture Fund require the completion of a specific form called a DEA-499 (Request for Payment). The DEA Special Agents Manual requires the "Remarks Section" of the DEA-103 to contain a brief synopsis of the basis or justification for the payment; identify the source of funds, if provided by another agency; and cite the investigative file document, source debriefing, or teletype that explains or justifies the payment. The DEA Special Agents Manual requires that the paper copies of the DEA-103s be maintained in the confidential source file.

The DEA Special Agents Manual also stipulates that all payments to confidential sources shall be commensurate with the value of the information provided or the assistance rendered. We found that the DEA provides its field offices broad discretion to determine how much to pay confidential sources.[39] According to field office Supervisory Special Agents, they are aware of the confidential sources' involvement in cases through regular contact with Special Agents handling the confidential sources so they do not always thoroughly examine all of the paperwork related to the justification for payment to the confidential sources. In general, we believe that this indicates that supervisors do not always conduct a careful review of documentation and justification for payments, which increases the risk that payments to confidential sources may not be appropriate.

We compared the DEA-103 forms to the CSSC payment information for 1,492 payments from 111 confidential source files. We found 289 instances (19 percent of the payments reviewed) in which the case number and payment reason on the DEA-103 forms did not match the information contained in CSSC. Also, the DEA Special Agents Manual states that payments for different purposes must be made on separate DEA-103 forms. Yet, we found 103 instances (7 percent of payments reviewed) wherein the DEA-103 forms listed multiple payment reasons.

Furthermore, we attempted to reconcile payments and the DEA-103 forms with documentation in the confidential source file, to include activity and debriefing reports that justified those payments. We found that some synopses on DEA-103 forms only referred to an investigative file document, debriefing report, or

[39] The current oversight structure allows Group Supervisors to approve individual non-award payments up to $2,500 and Assistant Special Agents in Charge (ASACs) to approve individual non-award payment amounts up to $25,000, which are the majority of payments to confidential sources. Any individual non-award payments above $25,000 must be approved by DEA's Special Agents in Charge (SACs) with the concurrence of the Chief of the Office of Operations Management or the Chief of International Operations. The Office of Operations Management also approves all field offices' requests for award payments to confidential sources, but field offices determine the percentage and amounts of award payments to confidential sources.

teletype rather than providing specific information to justify the payment. In some of these instances, we could not locate the investigative file document or debriefing report in the file and could not reconcile the payment with any justification. Other DEA-103 forms we reviewed included a vague statement about the confidential source's activities to justify payment, but did not refer to an investigative file document, debriefing report, or teletype, so we could not reconcile the payment to any case-related report or activity. Specifically, from our review of 1,492 payments to confidential sources, we found that 272 of those payments, or almost 17 percent, lacked appropriate justification.

Additionally, the DEA requires Special Agents to document on a DEA-103 the purpose of the reimbursement of expenses and, whenever possible, to attach a receipt to the DEA-103 to be included in the confidential source file.[40] If the Special Agent does not obtain a receipt from the confidential source, the Special Agent should provide an explanation of why a receipt was not obtained and included. We reviewed 111 confidential source files with a total of 134 confidential source payments associated with reimbursement for expenses. During this review, we found that 93 of 134 of these reimbursement payments, or 69 percent, had inadequate documentation or lacked sufficient justification for the DEA's payment of confidential source expenses.

The issues we found related to inadequate payment documentation and support are longstanding problems for the DEA. Some of these deficiencies were identified by the OIG in 2005 and by the DEA Inspections Division between FYs 2011 and 2015. However, the DEA has not implemented adequate internal controls and oversight mechanisms for confidential source payments to ensure that payments to confidential sources are justified and commensurate with the information and services provided. Therefore, we believe that the DEA should develop internal control and review procedures that include a thorough review and approval of the justification and documentation for confidential source payments.

[40] As shown in Table 3, confidential sources can be compensated for reasonable expenses incurred during investigation. Based upon our review of confidential source files, these expenses could include travel costs and assistance with living expenses such as rent and cellular telephones.

CONCLUSION AND RECOMMENDATIONS

According to the DEA, its Confidential Source Program is one of the most important aspects of DEA operations. DEA officials often refer to confidential sources as the "bread and butter" of the organization and say that confidential sources are critical to the DEA's pursuit of combating illegal narcotics trafficking. However, there are significant risks in using and paying confidential sources to assist in law enforcement activities, as these individuals are often associated with criminal activity and motivated by the potential for monetary compensation or consideration for a reduced criminal sentence. Effective management and oversight are imperative to optimizing the use of confidential sources, while also mitigating the risks associated with sources. We found that, despite these significant risks, the DEA's management of this program did not provide sufficient oversight and controls related to the DEA's establishment, use, and payment of confidential sources, in particular Limited Use and DEA intelligence-related sources.

We found that the DEA's reliance on Limited Use confidential sources to accomplish interdiction operations, the DEA's direction and guidance to these sources, and the DEA's long-term and lucrative relationships with these sources calls into question whether the source is truly providing information independently or is acting as DEA's agent, the latter of which could have implications relating to compliance with the Fourth Amendment's protections against unreasonable searches and seizures. However, neither the DEA, nor the Department, has comprehensively reviewed the use and payments to these sources for interdiction-related purposes.

In addition, although the DEA's Intelligence Division relies on the use of confidential sources to support intelligence-related programs and operations and allocates significant funding to pay confidential sources, it has not established sufficient oversight and control procedures to independently review sources and the information they provide, and to track payments made to these individuals. The DEA also has not established controls over the use of "sub-sources" by its confidential sources, which is a practice condoned by DEA Supervisory Special Agents and Special Agents that introduces significant risks for DEA and for the confidential sources themselves.

Further, the identification of administrative deficiencies related to the review and approval of confidential source information is indicative of weak program management. Inadequate documentation and insufficient internal controls and review processes, coupled with the broad discretion used by the field offices to determine payment amounts, are concerning because they increase the risk for fraud, waste, and abuse in the Confidential Source Program. Given the high frequency by which DEA offices utilize and pay confidential sources, there is a vital need for more robust oversight to mitigate these risks.

The totality of these deficiencies highlight significant concerns related to the adequacy of the current policies, procedures, and oversight associated with the

DEA's Confidential Source Program. We believe that the DEA should evaluate all aspects of its Confidential Source Program to ensure that it is managed effectively and consistently. As we concluded our audit work, we informed DEA management and program officials about our findings and concerns. These officials expressed a firm commitment to improve the Confidential Source Program, to implement appropriate controls over confidential sources, and to ensure that confidential sources remain a productive and essential element used by the DEA to accomplish its mission. To begin this process, we offer the following recommendations to help the DEA reengineer its Confidential Source Program.

We recommend that the DEA:

1. Examine the practices employed related to Limited Use confidential sources for interdiction operations as described in our report and, in coordination with the Department, perform an assessment of the risks, benefits, and legality of the practices.

2. Develop clear guidance and additional controls related to the appropriate use of the Limited Use confidential source category to ensure that these sources are used according to the category definition and receive appropriate oversight that is commensurate with the amount of compensation these sources are paid.

3. Establish controls to ensure complete and appropriate handling of documentation and tracking of interactions and information received from all confidential sources.

4. Develop and promulgate policy to prohibit DEA Special Agents from using unauthorized private correspondence (e.g., e-mail accounts, text messages) for government business, including interactions with confidential sources.

5. Examine the practices employed related to the use of confidential sources who provide intelligence-related information. The DEA should:

    a. Confer with the Department and the FBI to ascertain the need for procedures to implement an independent review of confidential sources to assess the reliability, authenticity, integrity, and overall value of a given source for intelligence-related purposes.

    b. Require the Intelligence Division to establish procedures to review intelligence-related information and services provided by confidential sources to ensure the requirements of the DEA's intelligence efforts are met.

    c. Ensure that the Intelligence Division adequately tracks all funds used for confidential source-related activities.

6. Evaluate the appropriateness of the use of “sub-sources” and determine if this practice should either be prohibited or formalized through the issuance of policies and procedures to mitigate associated risks.

7. Enhance the oversight and management of the Confidential Source Program, including measures to:

    a. Employ more frequent and rigorous confidential source management and oversight training to ensure consistent understanding and application of DEA policies.

    b. Address the consistency of confidential source categorization for sources with criminal histories and who are concurrently used by multiple DEA offices.

    c. Ensure controls over payments to deactivated sources include requirements for adequate justification and approval.

    d. Develop stricter internal controls for CSSC to ensure the consistency, accuracy, and completeness of information.

    e. Implement a reconciliation process to ensure payment records are accurate, complete, and consistent within the confidential source files, UFMS, and CSSC.

    f. Establish internal control and review processes at field offices to ensure consistent, thorough review of documentation and justification for confidential source payments.

    g. Evaluate the roles and responsibilities related to the management and administration of the Confidential Source Program, to ensure robust oversight of the establishment, use, and payments to confidential sources and to ensure that the field offices are consistently and thoroughly applying DEA policy and the AG Guidelines.

    h. Evaluate the headquarters-level use of CSSC for strategic, DEA-wide oversight and the review and monitoring of confidential source information.

STATEMENT ON INTERNAL CONTROLS

As required by *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of DEA's internal controls was not made for the purpose of providing assurance on the agency's internal control structures as a whole. DEA's management is responsible for the establishment and maintenance of internal controls.

Throughout our audit, we identified deficiencies in the DEA's internal controls that are significant within the context of the audit objectives. Based upon the audit work performed we believe the deficiencies identified adversely affect the DEA's ability to ensure that the Confidential Source Program is appropriately and adequately managed. These matters are discussed in detail in the Audit Findings section of this report.

Because we are not expressing an opinion on the DEA's internal control structure as a whole, this statement is intended solely for the information and use of the DEA. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

Government Auditing Standards require that we perform tests, as appropriate given our audit scope and objectives, to obtain reasonable assurance that DEA's management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. DEA's management is responsible for ensuring compliance with applicable federal laws and regulations applicable to the Department of Justice. Although we did not identify any federal laws or regulations that would apply specifically to the DEA's Confidential Source Program, we did identify such DOJ and DEA-level policies that we considered to be significant within the context of the audit objective, namely the Attorney General's Guidelines Regarding the Use of Confidential Informants and the DEA Special Agents Manual. Our audit included examining, on a test basis, DEA's compliance with the aforementioned policies that could have a material effect on the DEA's Confidential Source Program. We did so by examining applicable DEA confidential source policies, interviewing DEA and DOJ personnel, assessing internal control procedures and management practices, and reviewing confidential source files and payments.

As noted in the Introduction section of this report, we previously found that the DEA's policies for confidential sources were not congruent with the Attorney General's Guidelines Regarding the Use of Confidential Informants. Throughout this audit, the DEA has coordinated with the DOJ Criminal Division to update its policies to ensure compliance with the AG Guidelines. However, these policies were not implemented during the scope of our audit. As discussed in our report, we found that DEA's non-congruent policies and inadequate procedures related to its Confidential Source Program resulted in significant oversight and management deficiencies.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess the DEA's management and oversight of it Confidential Source Program, to include the DEA's oversight of payments to confidential sources. This audit is a continuation of work reported in the OIG's July 2015 report on *The DEA's Confidential Source Policies and Oversight of Higher-Risk Confidential Sources*. Our previous audit report included findings related to the examination of the DEA's confidential source policies to ensure consistency with the AG Guidelines requirements, reviewing the DEA's oversight of certain high-risk confidential sources and high-risk activities involving confidential sources, and evaluating the DEA's administration of death and disability benefits to confidential sources.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objective.

To accomplish our audit objective, we focused on DEA confidential sources who were ever active in any of the DEA's domestic offices from FY 2011 through FY 2015. We examined DEA confidential source data and conducted work at the following nine DEA field site locations: Albuquerque, New Mexico; Chicago, Illinois; El Paso, Texas; Los Angeles, California; Phoenix, Arizona; Sacramento, California; San Francisco, California; DEA Office of Special Intelligence; and the Special Operations Division.

We interviewed DOJ officials from the Office of the Deputy Attorney General, the Criminal Division, and two United States Attorneys' Offices. In addition, we interviewed DEA headquarters officials from the Office of Operations Management, Policy and Source Management Section, Confidential Source Unit, Inspections Division, Office of Professional Responsibility, Intelligence Division, Office of Special Intelligence, Office of Finance, Office of Security Programs, Office of Information Systems, and Office of Chief Counsel. We also interviewed field office and Special Operations Division personnel, including Special Agents, Task Force Officers, Group Supervisors, Assistant Special Agents in Charge, and Confidential Source Coordinators. In total, we interviewed more than 50 DEA and DOJ officials.

CSSC Data Reliability Testing, Analysis, and Utilization

We coordinated with the DEA's Confidential Source Unit and Office of Information Systems and requested that the DEA provide the OIG with a data file

containing records for all confidential sources that were ever active in any DEA domestic office between FY 2011 and FY 2015, as tracked in the Confidential Source System Concorde (CSSC). The DEA provided an electronic file that contained CSSC data related to the establishment, risk assessment, annual certification, deactivation, and payments for 18,726 confidential sources. We reviewed the DEA's requirements for confidential source forms and payment information to verify completeness, accuracy, and reliability of the data file we received from the DEA. We identified that certain required fields did not have complete, consistent, and reliable information. Specifically, we found null and invalid values in fields such as occupation, employer name, establishment approval date, and criminal history. Although these fields are expected to be filled out by Special Agents, DEA officials explained that CSSC allows for exceptions, which result in blank values, in the event that the confidential source is unemployed or established for the purpose of a special payment. According to DEA officials, the system controls in CSSC were not designed to prohibit Special Agents from not entering information in required fields and, therefore, CSSC allows Special Agents to hit the space bar to skip certain fields that they do not want to include or do not have the information needed to complete. Officials from the DEA's Office of Information Systems stated that CSSC controls could be enhanced to ensure that information is entered in a complete and consistent method.

In addition, through our data analysis and confidential source file testing, we found that payment data was duplicated, missing, or inaccurate. DEA officials stated that these deficiencies were generally caused by weak internal controls and the absence of a reconciliation process between CSSC, the confidential source files, and the Unified Financial Management System. In addition, DEA officials found that the methodology used by the DEA's Office of Information Systems to generate our data file, as requested by the OIG, resulted in the creation of erroneous duplicate information. In order to ensure data accuracy, the DEA tried to identify and delete these duplicate errors in our data file, but, mistakenly also excluded some valid payments because they were misidentified as erroneous duplicates. We worked with the DEA to identify the universe of missing payments but we cannot be assured that all were identified.

As a result of these weaknesses, we could not fully rely on the CSSC data file to provide statistical information upon which we could base audit conclusions. However, because this was the only data available to the OIG during the scope of our audit related to the DEA's Confidential Source Program, we conducted data summary analysis, as identified in the following section, to select DEA offices for field site visits, to identify areas of risk for further review, and to contribute to the corroboration of certain issues identified through other analysis.

Data Analysis, Field Site Selection, and Confidential Source File Testing

We used the DEA's CSSC data to identify sources in the following categories that we assessed to be high-risk: confidential sources identified as requiring special approval, confidential sources with high-risk employment, confidential sources with large payments, and confidential sources with high frequency of

payments. We analyzed the CSSC data file to determine how much money the DEA paid to the 18,726 domestically used confidential sources during the scope of our review. According to the data, the DEA paid 9,540 sources approximately $237 million between FY 2011 and FY 2015.

We judgmentally selected a sample of 120 confidential sources for detailed review; these sources were paid more than $36 million during our review period. The source files that we reviewed were located in the following offices: Albuquerque, New Mexico; Chicago, Illinois; El Paso, Texas; Los Angeles, Sacramento, and San Francisco, California; Phoenix, Arizona; DEA Office of Special Intelligence; and the Special Operations Division. In addition, we reviewed a sample of 19 investigative case files that were associated with some of the confidential sources in our source sample. Our sample selection methodologies were not designed with the intent of projecting our results to the population from which the samples were selected.

THE DRUG ENFORCEMENT ADMINISTRATION'S RESPONSE TO THE DRAFT AUDIT REPORT

U. S. Department of Justice
Drug Enforcement Administration

www.dea.gov Washington, D.C. 20537

SEP 2 3 2016

MEMORANDUM

TO: Carol S. Taraszka
Regional Audit Manager
Chicago Regional Audit Office
Office of the Inspector General

FROM: Michael J. Stanfill
Deputy Chief Inspector
Office of Inspections

SUBJECT: Drug Enforcement Administration's Response to the OIG Draft Report, *"The Drug Enforcement Administration's Management and Oversight of Its Confidential Source Program"*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ) Office of the Inspector General's (OIG) September 2016 Draft Report entitled, "*The Drug Enforcement Administration's Management and Oversight of Its Confidential Source Program.*" DEA acknowledges and appreciates OIG's efforts in conducting a review to assess DEA's management and oversight of the Confidential Source (CS) Program to ensure that the risks posed by the use of CSs are appropriately handled.

Confidential sources provide invaluable contributions and assistance to DEA investigations. However, DEA recognizes the inherent risk involved when relying on persons whose motivations can be suspect. Thus, steps have been taken to mitigate identified risks.

Since the issuance of OIG's previous report in July 2015 regarding DEA's CS policies and its oversight of higher-risk CSs, DEA has worked with the DOJ Criminal Division and the Office of the Deputy Attorney General to develop clear policy in compliance with the Attorney General's Guidelines regarding the use of Confidential Informants (AG Guidelines). In July 2016, DEA issued new policy that addresses most of the OIG's concerns in the prior report and current draft report. However, DEA continues to review the program to identify areas for improvement, clarification, and stricter guidelines.

The OIG provided seven recommendations in the report and DEA concurs with each recommendation. Below are DEA's responses to the recommendations.

Recommendation 1: Examine the practices employed related to Limited Use confidential sources for interdiction operations as described in our report and, in coordination with the Department, perform an assessment of the risks, benefits, and legality of the practices.

DEA Response

DEA acknowledges issues raised in the Report concerning the practices employed related to the use of Limited Use CSs for interdiction operations. For the past several months, DEA Executive Management has been reviewing its policies governing Limited Use CSs and, in coordination with the Department, will adopt or amend policies as appropriate to address these concerns and ensure that all practices are consistent with the AG Guidelines.

Recommendation 2: Develop clear guidance and additional controls related to the appropriate use of the Limited Use confidential source category to ensure that these sources are used according to the category definition and receive appropriate oversight that is commensurate with the amount of compensation these sources are paid.

DEA Response

See response to Recommendation 1.

Recommendation 3: Establish controls to ensure complete and appropriate handling of documentation and tracking of interactions and information received from all confidential sources.

DEA Response

DEA has issued global notifications of the revised CS polices in order to ensure awareness among DEA's workforce and to provide clear guidance and controls related to the appropriate use of the Limited Use CS category. Formal Confidential Source Coordinator (CSC) training has been conducted to ensure complete and appropriate handling of documentation, tracking, and information received from all CSs. The training has been identified as annual training. Documentation of the training has been provided to OIG under separate cover.

Based on these actions, DEA requests closure of this recommendation upon issuance of the final report.

Recommendation 4: Develop and promulgate policy to prohibit DEA Special Agents from using unauthorized private correspondence (e.g., e-mail accounts, text messages) for government business, including interactions with confidential sources.

DEA Response

DEA policy currently requires that Special Agents preserve communications with CSs, regardless of the method of such correspondence. DEA's Office of Investigative Technology, in conjunction with other DEA offices, is exploring methods to improve DEA's operational security, vulnerability awareness and training, and evidence retention when interacting with CSs through electronic means. Once methods and best practices are identified, these guidelines will be formalized into agency policy to ensure compliance in utilizing only authorized modes of correspondence when interacting with CSs.

Recommendation 5: Examine the practices employed related to the use of confidential sources who provide intelligence-related information. The DEA should:

a. Confer with the Department and the FBI to ascertain the need for procedures to implement an independent review of confidential sources to assess the reliability, authenticity, integrity, and overall value of a given source for intelligence-related purposes.

DEA Response

Executive Management is consulting with the FBI to discuss their methodology relative to CSs. DEA will compare FBI's methodology with DEA procedures and evaluate the applicability to DEA's mission.

b. Require the Intelligence Division to establish procedures to review intelligence-related information and services provided by confidential sources to ensure the requirements of the DEA's intelligence efforts are met.

DEA Response

The Intelligence Division is developing formal standard operating procedures to review intelligence-related information and services provided by CSs.

c. Ensure that the Intelligence Division adequately tracks all funds used for confidential source-related activities.

DEA Response

The standard operating procedures noted in recommendation 5b above will also address tracking funds used for intelligence CS related activities.

Recommendation 6: Evaluate the appropriateness of the use of "sub-sources" and determine if this practice should either be prohibited or formalized through the issuance of policies and procedures to mitigate associated risks.

DEA Response

DEA currently is reviewing its policies and practices on the use of sub-sources. As part of that review, DEA Executive Management is consulting with the FBI to discuss their methodology relative to CSs and the use of sub-sources. DEA will compare FBI's methodology with DEA procedures and evaluate the applicability to DEA's mission and, in coordination with the Department, will adopt or amend policies as appropriate to ensure all practices are consistent with the AG Guidelines.

Recommendation 7: Enhance the oversight and management of the Confidential Source Program, including measures to:

a. Employ more frequent and rigorous confidential source management and oversight training to ensure consistent understanding and application of DEA policies.

b. Address the consistency of confidential source categorization for sources with criminal histories and who are concurrently used by multiple DEA offices.

c. Ensure controls over payments to deactivated sources include requirements for adequate justification and approval.

d. Develop stricter internal controls for CSSC to ensure the consistency, accuracy, and completeness of information.

e. Implement a reconciliation process to ensure payment records are accurate, complete, and consistent within the confidential source files, UFMS, and CSSC.

f. Establish internal control and review processes at field offices to ensure consistent, thorough review of documentation and justification for confidential source payments.

g. Evaluate the roles and responsibilities related to the management and administration of the Confidential Source Program, to ensure robust oversight of the establishment, use, and payments to confidential sources and to ensure that the field offices are consistently and thoroughly applying DEA policy and the AG Guidelines.

h. Evaluate the headquarters-level use of CSSC for strategic, DEA-wide oversight and the review and monitoring of confidential source information.

DEA Response

In addition to publishing a revised CS policy in July 2016, a corresponding global message was also broadcast in July 2016, to highlight "notable changes" to the CS policy, to instruct personnel to review the revised policy, and to provide notification of a new requirement for CS documentation relative to accuracy and completeness of the establishment form (DEA-512). Formal CSC training began in September 2016, at the DEA Academy to ensure more frequent and rigorous management and oversight training occurs, and to foster greater understanding and

consistent application of policies. The training also focuses on the assurance that adequate justification and approval for payments to deactivated CSs have controls in place.

DEA's Office of Inspections has also revised the CS checklists for utilization during the inspection process to ensure compliance by DEA field offices regarding the newly implemented policy directivess. The checklists have been provided to OIG under separate cover.

Executive management continues to discuss ways to further evaluate and enhance DEA's oversight, effectiveness, and consistency relative to the overall management and oversight of the CS program.

Based on these actions, DEA requests closure of recommendations 7a, b, c, and f upon issuance of the final report.

Thank you for the opportunity to respond to the recommendations made in the OIG report. If you have any questions regarding this response, please contact the Audit Liaison Team, on 202-307-8200.

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

The OIG provided a draft of this audit report to the DEA. The DEA's response is incorporated in Appendix 2 of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendations to the DEA:

1. **Examine the practices employed related to Limited Use confidential sources for interdiction operations as described in our report and, in coordination with the Department, perform an assessment of the risks, benefits, and legality of the practices.**

   Resolved. The DEA concurred with our recommendation. The DEA's response acknowledges issues raised in the report related to the use of Limited Use confidential sources for interdiction operations. The DEA stated that DEA Executive Management has been reviewing the policies governing Limited Use confidential sources and, in coordination with the Department, will adopt or amend policies as appropriate to address these concerns and ensure that all practices are consistent with the Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines).

   This recommendation can be closed when we receive evidence that the DEA has examined practices employed related to Limited Use confidential sources for interdiction operations as described in our report and, in coordination with the Department, performed an assessment of the risks, benefits, and legality of the practices.

2. **Develop clear guidance and additional controls related to the appropriate use of the Limited Use confidential source category to ensure that these sources are used according to the category definition and receive appropriate oversight that is commensurate with the amount of compensation these sources are paid.**

   Resolved. The DEA concurred with our recommendation. The DEA referred to its response for Recommendation 1, which acknowledged issues raised in the report concerning the DEA's use of Limited Use confidential sources for interdiction operations. The DEA stated that DEA Executive Management has been reviewing its policies governing Limited Use confidential sources and, in coordination with the Department, will adopt or amend policies as appropriate to address these concerns and ensure that all practices are consistent with the AG Guidelines.

This recommendation can be closed when we receive evidence that the DEA has developed clear guidance and additional controls related to the appropriate use of the Limited Use confidential source category to ensure that these sources are used according to the category definition and receive appropriate oversight that is commensurate with the amount of compensation these sources are paid.

3. **Establish controls to ensure complete and appropriate handling of documentation and tracking of interactions and information received from all confidential sources.**

   Resolved. The DEA concurred with our recommendation. The DEA stated in its response that it notified all of its employees of the revised confidential source policies in order to ensure awareness within the DEA's workforce and to provide clear guidance and controls related to the appropriate use of the Limited Use confidential source category. In addition, the DEA stated that formal Confidential Source Coordinator training has been initiated to ensure complete and appropriate handling of documentation, tracking, and information received from all sources. The DEA stated that it has identified this training as annual training and provided the OIG with the training documentation.

   The DEA requested closure of this recommendation based on these actions. However, based on the OIG's review of the documentation provided by the DEA, we do not believe that this recommendation has been fully addressed. While the DEA provided its workforce with clear and specific guidance related to revised confidential source policies that were issued in July 2016, these new policies primarily addressed the recommendations from our July 2015 report and the DEA's more recent prohibition to establish as confidential sources government or quasi-government employees, to include Amtrak and Transportation Security Administration personnel. However, the revised confidential source policies do not include specific instructions related to the appropriate handling of documentation and tracking of interactions and information received from all confidential sources.

   This recommendation can be closed when we receive evidence that the DEA has established controls to ensure complete and appropriate handling of documentation and tracking of interactions and information received from all confidential sources.

4. **Develop and promulgate policy to prohibit DEA Special Agents from using unauthorized private correspondence (e.g., e-mail accounts, text messages) for government business, including interactions with confidential sources.**

   Resolved. The DEA concurred with our recommendation. The DEA stated in its response that DEA policy currently requires that Special Agents preserve communications with confidential sources, regardless of the method of such correspondence. Further, the DEA's Office of Investigative Technology, in conjunction with other DEA offices, is exploring methods to improve the DEA's operational security, vulnerability awareness and training, and evidence retention when interacting with confidential sources through electronic means. The DEA stated that once methods and best practices are identified, guidelines will be formalized into DEA policy to ensure compliance in utilizing only authorized modes of correspondence when interacting with sources.

   This recommendation can be closed when we receive evidence that the DEA has developed and promulgated policy to prohibit DEA Special Agents from using unauthorized private correspondence (e.g., e-mail accounts, text messages) for government business, including interactions with confidential sources.

5. **Examine the practices employed related to the use of confidential sources who provide intelligence-related information. The DEA should:**

   a. **Confer with the Department and the FBI to ascertain the need for procedures to implement an independent review of confidential sources to assess the reliability, authenticity, integrity, and overall value of a given source for intelligence-related purposes.**

   Resolved. The DEA concurred with our recommendation. The DEA stated in its response that DEA Executive Management is consulting with the FBI to discuss its methodology relative to confidential sources. The DEA stated that it will compare the FBI's methodology with the DEA's procedures and evaluate the applicability to the DEA's mission.

   This recommendation can be closed when we receive evidence that the DEA conferred with the Department and the FBI to ascertain the need for an independent review of confidential sources to assess the reliability, authenticity, integrity, and overall value of a given source for intelligence-related purposes.

b. Require the Intelligence Division to establish procedures to review intelligence-related information and services provided by confidential sources to ensure the requirements of the DEA's intelligence efforts are met.

Resolved. The DEA concurred with our recommendation. The DEA stated in its response that the DEA Intelligence Division is developing formal standard operating procedures to review intelligence-related information and services provided by confidential sources.

This recommendation can be closed when we receive evidence that the DEA's Intelligence Division has established procedures to review intelligence-related information and services provided by confidential sources to ensure the requirements of the DEA's intelligence efforts are met.

c. Ensure that the Intelligence Division adequately tracks all funds used for confidential source-related activities.

Resolved. The DEA concurred with our recommendation. The DEA stated in its response that the standard operating procedures noted in Recommendation 5b will also address tracking funds used for intelligence-related confidential sources.

This recommendation can be closed when we receive evidence that the DEA's Intelligence Division is adequately tracking all funds used for confidential source-related activities.

6. Evaluate the appropriateness of the use of "sub-sources" and determine if this practice should either be prohibited or formalized through the issuance of policies and procedures to mitigate associated risks.

Resolved. The DEA concurred with our recommendation. The DEA stated in its response that it is currently reviewing its policies and practices on the use of sub-sources. The DEA stated that as part of the review, DEA Executive Management is consulting with the FBI to discuss its methodology relative to confidential sources and the use of sub-sources. The DEA will compare the FBI's methodology with DEA procedures and evaluate the applicability to the DEA's mission and, in coordination with the Department, adopt or amend policies as appropriate to ensure all practices are consistent with the AG Guidelines.

This recommendation can be closed when we receive evidence that the DEA has evaluated the appropriateness of the use of "sub-sources" and determined if this practice should either be prohibited or formalized through the issuance of policies and procedures to mitigate associated risks.

7. **Enhance the oversight and management of the Confidential Source Program, including measures to:**

    a. **Employ more frequent and rigorous confidential source management and oversight training to ensure consistent understanding and application of DEA policies.**

    b. **Address the consistency of confidential source categorization for sources with criminal histories and who are concurrently used by multiple DEA offices.**

    c. **Ensure controls over payments to deactivated sources include requirements for adequate justification and approval.**

    d. **Develop stricter internal controls for CSSC to ensure the consistency, accuracy, and completeness of information.**

    e. **Implement a reconciliation process to ensure payment records are accurate, complete, and consistent within the confidential source files, UFMS, and CSSC.**

    f. **Establish internal control and review processes at field offices to ensure consistent, thorough review of documentation and justification for confidential source payments.**

    g. **Evaluate the roles and responsibilities related to the management and administration of the Confidential Source Program, to ensure robust oversight of the establishment, use, and payments to confidential sources and to ensure that the field offices are consistently and thoroughly applying DEA policy and the AG Guidelines.**

    h. **Evaluate the headquarters-level use of CSSC for strategic, DEA-wide oversight and the review and monitoring of confidential source information.**

Resolved. The DEA concurred with our recommendation. The DEA stated in its response that in addition to publishing a revised confidential source policy in July 2016, a corresponding global message was also broadcast to all personnel to highlight "notable changes" to the confidential source policy, instruct personnel to review the revised policy, and provide notification of a new requirement for confidential source documentation relative to accuracy and completeness of the source establishment form. In addition, the DEA stated that formal Confidential Source Coordinator training began in September 2016 to ensure more frequent and rigorous management and oversight training occurs, and to foster greater understanding and consistent

application of policies. The DEA stated that its Executive Management continues to discuss ways to further evaluate and enhance the DEA's oversight, effectiveness, and consistency relative to the overall management and oversight of the Confidential Source Program. As a result of these actions, the DEA requested that the OIG close recommendations 7a, b, c, and f, upon issuance of the final report.

The OIG reviewed the DEA's response and corresponding documentation and we do not believe that we can close these subparts of recommendation 7 at this time. The DEA has taken important first steps in employing more rigorous confidential source management and oversight training by providing training to its Confidential Source Coordinators and making this training an annual requirement. However, recommendation 7a, to employ more frequent and rigorous confidential source management and oversight training to ensure consistent understanding and application of DEA policies, also applies to DEA Special Agents, supervisors, and managers who are responsible for executing the confidential source policies and requirements. Therefore, we believe that the DEA should determine how it may provide these employees with additional and more frequent Confidential Source Program training.

Specific to recommendation 7b, which relates to the consistency of confidential source categorization for sources with criminal histories and who are concurrently used by multiple DEA offices, the DEA provided the updated confidential source policy that now requires Senior Executive Service (SES) mangers from concurrent use offices to coordinate the establishment and utilization of a confidential source by both offices. However, based on our review of the documentation that the DEA provided, there is no specific guidance that addresses our identification of occurrences of inconsistent categorization of Limited Use confidential sources with criminal histories. Moreover, as noted in recommendations 1 and 2, policies governing Limited Use sources are under DEA Executive Management review.

For recommendation 7c, which recommends that the DEA ensure controls over payments to deactivated sources include requirements for adequate justification and approval, the DEA stated that the training provided to Confidential Source Coordinators focused on the assurance that adequate justification and approval for payments to deactivated sources have controls in place. However, the training documentation the DEA provided to the OIG did not contain evidence that the DEA had reevaluated the controls over payments to deactivated sources or reinforced to Confidential Source Coordinators the requirements for adequate justification and approval of such payments.

Finally, in response to recommendation 7f, to establish internal control and review processes at field offices to ensure consistent, thorough review of documentation and justification for confidential source payments, the DEA stated that the Office of Inspections has revised the confidential source

checklists utilized during the inspections process to ensure field office compliance with the newly implemented policy directives. The DEA provided these checklists to the OIG during the audit and based on our review, we believe that the updated checklist demonstrates an improvement in this compliance area, as it requires inspectors to identify if documentation to support payments is contained in the confidential source file and if the payments in the source file correspond to the data contained in CSSC. However, we found that this checklist does not provide instructions or a requirement to thoroughly review and assess DEA field offices' justification for confidential source payments to ensure that all payments are appropriate and supported.

For the above-mentioned reasons, the OIG believes that this recommendation, in its entirety, should remain open. The DEA's response indicates that DEA Executive Management continues to discuss ways to further evaluate and enhance the oversight, effectiveness, and consistency relative to the overall management and oversight of the DEA's Confidential Source Program. We look forward to the results of this evaluation and the resulting enhancements in the DEA's management and use of confidential sources. This recommendation can be closed when we receive evidence that the DEA has enhanced the oversight and management of the Confidential Source Program, including measures to address all subparts of this recommendation.

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig