



Audit of the Department of Justice Components' Confidential Informant Policies



AUDIT DIVISION

27-003

OCTOBER 2026



Audit of the Department of Justice Components' Confidential Informant Policies

Introduction

The Department of Justice's (Department or DOJ) law enforcement components—the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); and U.S. Marshals Service (USMS)—use confidential informants (CI), or individuals who provide useful and credible information to law enforcement on a continuing basis, to assist in accomplishing their missions.¹ The use of CIs is a powerful law enforcement tool that also presents an inherent risk to the Department due to CIs' potential affiliation with illegal activities and cooperation motivated by compensation or other benefits. To mitigate the risks of using CIs, DOJ has established Department-wide operational guidance.

Audit Objective

The objective of our audit was to review Attorney General guidance on the use of CIs and assess whether each DOJ law enforcement component's policies complied with the appropriate Department guidance. This audit focused on the content of component policies. We reviewed Department and component policies and met with component headquarters officials who oversee the administration of CI programs. Appendix 1 contains further details on our audit objective, scope, and methodology.

Results in Brief

We found that all components' policies, procedures, and training substantially complied with applicable Attorney General guidance; however, each component needs to make certain updates to fully comply with Department guidance. Further, DOJ should revisit its policies to address additional risks stemming from evolving law enforcement

priorities and techniques, such as designating cartels and other organizations as foreign terrorist organizations, designating fentanyl as a weapon of mass destruction, information sharing, and monetary payments to CIs. Additionally, in reviewing and comparing the two Attorney General Guidelines that apply to different components, we found DOJ has not been entirely consistent in its internal control requirements for all components, which leads to varying levels of oversight.

Conclusion and Recommendations

Guidance that does not address evolving law enforcement priorities and techniques and non-compliance with the Department's policies increases the risk that DOJ law enforcement officers will fail to adhere to critical controls designed to minimize inherent risks associated with overseeing CIs. These risks include the furtherance of criminal activity and threat to public safety; the risk that CI affiliation with illicit activity may result in personal gain or abuse of the CI program; and waste of taxpayer funds.

We make five recommendations in this report, including one to the Department to establish controls for helping address emerging risks associated with the use of CIs and to account for differences in component frameworks. The remaining recommendations are provided to ATF, the DEA, the FBI, and the USMS to enhance their CI-related policies to ensure compliance with Department guidance. The components concurred with our recommendations in response to a draft of this report; these responses can be found in Appendices 3 through 7. Our analysis of those responses and actions needed to close the report can be found in Appendix 8.

¹ DOJ law enforcement components use different terms to refer to individuals believed to be providing useful and credible information to law enforcement, and from whom the agency expects or intends to obtain additional useful and credible information in the future. For purposes of this report, we use the term confidential informant (CI), which is used by the Department in the Attorney General's Guidelines Regarding the Use of Confidential Informants, as all encompassing.

Department-wide Audit Results

Department-wide CI Guidance Should be Updated

DOJ has issued Department-wide operational guidance that establishes the internal control framework over CIs, undercover activity, and other law enforcement matters. This guidance includes the Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines CI), the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources (AG Guidelines FBI CHS), and the "Baseline Risk Assessment and Mitigation Policies for Law Enforcement Operations in Criminal Matters" Memorandum (Risk Assessment Memo) issued by former Deputy Attorney General James M. Cole.² To decrease operational risks and safeguard taxpayer funds, DOJ's law enforcement components are required to operate within these guidelines by implementing internal controls that include formal policies, information systems, and training.

We reviewed the AG Guidelines CI (which apply to ATF, the DEA, and the USMS), the AG Guidelines FBI CHS (which apply to the FBI), and the Risk Assessment Memo (which apply to all DOJ law enforcement components) to identify the internal control framework for the use of CIs and found that collectively they contain numerous policy and process requirements, categorized in Figure 1.

We found that the Department's internal controls adequately account for the stages of using a CI and that the framework provides requirements for law enforcement components to

develop comprehensive policies, financial processes, and training to reinforce those controls. However, our comparison of the AG Guidelines CI and the AG Guidelines FBI CHS identified some differences, such as management reporting of otherwise illegal activity (OIA) conducted by CIs and oversight of CIs working in foreign intelligence or foreign counterintelligence matters. Moreover, we found that Department guidance has not adequately addressed significant changes to law enforcement operations, including risks related to recent Executive Orders, the transition from cash-based to electronic payments, management oversight of OIA, and the approval and use of certain high-level CIs.³

These differences may have resulted from distinct component missions or the timeframe in which each set of guidelines was drafted. The AG Guidelines CI was last updated in 2002, the Risk Assessment Memo was issued in 2013, and the AG Guidelines FBI CHS was last updated in 2020. Office of the Deputy Attorney General (ODAG) personnel did not identify any additional substantive guidance for all components since the Risk Assessment Memo was issued. We believe the Department should periodically update its policies to reflect changes in the operating environment and investigative methods. Doing so would better position the Department to provide current and consistent guidance to its law enforcement components. Absent such updates, components may revise CI policies and practices in different ways, which could result in inconsistencies in CI program management and in how safety considerations for CIs and the public are addressed.

Figure 1

Department's Confidential Informant Internal Control Framework

1. Identification and selection of CIs
2. Professional responsibilities for interacting with CIs
3. Management review and approval for the use of CIs
4. Safeguards over payments and other benefits provided to CIs
5. Precautions over the use of OIA conducted by CIs
6. Coordination with stakeholders, such as prosecutors and state/local law enforcement
7. Training on Department guidance
8. Approvals associated with foreign operations
9. Deactivation of CIs

Source: Office of the Inspector General (OIG) analysis of Department Guidance

² In 2006, the FBI and the Department worked to update guidelines for the FBI's use of sources that would enhance the FBI's ability to share human intelligence within its organization as a result of the *Intelligence Reform and Terrorism Prevention Act*, Public Law 108-458. The AG Guidelines FBI CHS were last updated in 2020.

³ Executive Order (E.O.) 14157 on Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists (E.O. 14157); Executive Order 14367 on Designating Fentanyl as a Weapon of Mass Destruction (E.O. 14367).

Changes Resulting from Recent Executive Orders

Recent Executive Orders have implications across multiple DOJ components. In particular, the Executive Order designating drug cartels as foreign terrorist organizations (E.O. 14157) and the Executive Order designating fentanyl as a weapon of mass destruction (E.O. 14367) shift narcotics trafficking from a traditional law enforcement environment to a national security environment. As a result, the missions of combatting illicit drugs and guns from cartels designated as foreign terrorist organizations, as well as pursuing such individuals, or fugitives, cause ATF, the DEA, and the USMS to operate in or adjacent to the national security environment.

The AG Guidelines CI do not apply to the use of CIs in foreign intelligence or foreign counterintelligence investigations (i.e., in a national security environment) and therefore ATF, the DEA, and the USMS do not have any guidance to govern their use of CIs in matters covered by these Executive Orders.⁴ ODAG acknowledged that the shift from law enforcement to national security has implications for law enforcement techniques that should be contemplated, and thus commissioned a review of the potential implications for national security information sharing. While ATF and DEA personnel told us that they continue to employ the same law enforcement strategies as before the issuance of the Executive Orders, we are concerned that the AG Guidelines CI may not contain appropriate safeguards to protect CIs and share and preserve information within the U.S. Intelligence Community.

Changes to Payment Strategies

CI payments have historically been cash-based. Our review of Department guidance found that the AG Guidelines CI do not contemplate the use of electronic payments, and the AG Guidelines FBI CHS allow for electronic payments only in extraordinary circumstances without any further internal controls to govern the process. However, several law enforcement components stated that they have used electronic payments with CIs, and we found that some of their policies cover electronic payments. FBI personnel, in particular, recognized the importance of electronic payments as a means of paying CIs. Yet, the Department has not issued guidance to establish its accepted level of risk and expected internal controls related to electronic banking and virtual transactions. Further, FBI personnel noted that alternative payment methods, such as cryptocurrency, may be an effective way to pay CIs that is currently not contemplated under the AG Guidelines FBI CHS. For example, current

guidance does not consider certain risks associated with the involvement of commercial banks in sensitive government bank transactions. To effectively respond to these risks, the Department should evaluate electronic payment mechanisms that could be used to pay CIs, while safeguarding funds and protecting operational integrity.

Management Oversight of OIA

OIA performed by CIs and overseen by law enforcement officers is an extremely powerful tool for gathering evidence. Because OIA involves authorizing a CI to engage in criminal activity and may result in harm to other persons or property, this investigative tool requires careful oversight. Both the AG Guidelines FBI CHS and AG Guidelines CI establish internal controls over the review and approval process for a CI performing OIA. The FBI must report data to the Department on all OIA annually as required by the AG Guidelines FBI CHS; however, ATF, the DEA, and the USMS are not subject to this annual reporting requirement. Reporting OIA data consistently to the Department provides transparency and the opportunity to assess its risk tolerance of Department-authorized criminal activity. Without requiring ATF, the DEA, and the USMS to report on OIA, the Department lacks consistent and complete oversight of OIA use by its law enforcement components.

Management Approval of High-Level CIs

At times, law enforcement engages with certain CIs who require careful legal review and risk assessment prior to use, otherwise referred to as high-level CIs, because of how closely these individuals are associated with criminal enterprises or because of their affiliation with protected speech. The AG Guidelines CI require Confidential Informant Review Committee (CIRC) approval prior to CI operations using high-level CIs.⁵ The AG Guidelines FBI CHS allow for the FBI to use certain CIs (those designated as high-level or affiliated with media or legal privilege) for 60 days prior to full approval by its CIRC. As a result, the AG Guidelines FBI CHS create the potential for using a high-level CI for a period of less than 60 days without obtaining CIRC approval, when the same use of a high-level CI would require ATF, the DEA, and the USMS to first obtain CIRC approval in accordance with the AG Guidelines CI.

Information Sources Not Subject to the AG Guidelines CI

DEA and USMS policies include a category of sources who provide, and are paid for, information but who are not subject to the full AG Guidelines CI because the individuals

⁴ The Intelligence Community (IC) provides guidance related to the use of CIs for national security operations intended to protect the national defense and foreign relations of the United States through various IC Directives.

⁵ Each component uses a different name for the group of supervisors, headquarters personnel, and Department representatives that review decisions related to the registration and utilization of CIs. For purposes of this report, we refer to this committee as the Confidential Informant Review Committee.

are not categorized as CIs. For instance, the DEA's policy categorizes certain individuals as "Limited-Use" sources when these individuals, without direction from the DEA, provide the DEA with information they possess or have access to as part of their occupations or routines (but not as a result of any criminal association). Further, USMS personnel believe these sources of information are different from CIs because these sources generally provide information only about fugitive locations, do not perform OIA, and do not provide evidence in court.

We acknowledge the DEA and USMS's justifications for distinguishing sources of information from CIs and the potential operational impact that additional requirements could have on the relationship between the DEA or the USMS and such sources of information. However, the use of these sources of information is not subject to all of the required AG Guidelines CI practices that are designed to help mitigate risks with managing CIs. Previous OIG oversight has identified risks and gaps associated with the use and management of sources of information.⁶ We believe that ODAG, when reviewing the AG Guidelines, is best positioned to weigh the benefits of requiring sources of information to maintain full compliance with AG Guidelines (as is required of CIs), by which the DEA and the USMS would be made aware of important risks such as status changes of sources of information, adverse actions taken by these sources, or these sources' development of criminal associations, against the impact on DEA and USMS operations.

Views of Department Leadership

We discussed with ODAG personnel the need to update Department guidance to consider the effects of recent Executive Orders, the prevalence of electronic payments, annual reporting requirements for CIs performing OIA, and management approval of high-level CIs. In response, an ODAG official said that it would be prudent to convene a working group consisting of representatives from the law enforcement components to update Department guidance. Such a working group could evaluate policy differences, current CI practices and risks, the use of sources of

information, and internal controls within CI programs to ensure the Department's CI governance framework sufficiently addresses existing and emerging law enforcement topics.

Component-Specific Audit Results

Components Require Policy and Procedure Improvements

The OIG has conducted prior work relevant to CIs across DOJ law enforcement components, acknowledging the inherent risk that comes with using CIs and identifying concerns, such as inappropriate CI and controlling agent relationships, non-compliance with AG Guidelines, inadequate vetting practices, and improper use of special CI categories, as shown in Appendix 2. In continuing this work, we assessed DOJ law enforcement component policies and practices to determine if they included the Department's internal control requirements as articulated in the AG Guidelines CI, AG Guidelines FBI CHS, and Risk Assessment Memo.

Overall, DOJ law enforcement components largely adhered to the relevant Department guidance regarding the establishment of internal controls to protect CI identities, mitigating risks associated with working with CIs linked to criminal organizations, and safeguarding funds. However, as illustrated in Figure 2, there are opportunities for each component to enhance its policy framework to more closely align with Department-level requirements. Of particular importance, we identified areas of improvement for monitoring CIs performing OIA and necessary enhancements to administrative processes that, when implemented, will result in the components' policies being in full compliance with existing Department guidance.

We informed each component of the policy differences we identified so each component can ensure its policies are in full compliance with Department guidance, as outlined in Figure 2. Several components acknowledged that they could improve their frameworks with respect to these areas. The areas where we identified necessary policy revision are discussed below.

⁶ See Appendix 2 for an overview of the OIG's CI-related oversight.

Figure 2
OIG Evaluation of Component CI Policies

	Internal Controls	ATF	DEA	FBI	USMS	Issues Identified
	Initial Suitability	+	✓	✓	✓	ATF does not list all initial suitability criteria in policy but includes most criteria in its forms.
	Responsibilities and Required Actions	+	✓	+	+	FBI policy should clarify circumstances for sharing CI relationship or inappropriate socialization information with federal prosecutors, while ATF and the USMS did not include the policy requirements associated with findings related to OIA and Training, as discussed below.
	Management Oversight and Approvals	+	+	✓	✓	ATF policy does not fully reflect all high-level review requirements. DEA policy does not include all requirements to use parolee participants.
	Payments and Other Benefits	✓	✓	✓	+	USMS payment practices place them at risk for fraud, waste, and abuse. See <i>USMS Payment Process</i> below.
	Otherwise Illegal Activity	+	+	✓	+	ATF , DEA , and USMS policies do not require the consideration of the impact of CIs interacting with dangerous commodities, such as firearms. See <i>Considerations for CIs Performing OIA</i> below.
	Coordination with Stakeholders	✓	✓	+	✓	As noted in Responsibilities and Required Actions above, the FBI should clarify certain due diligence reporting to federal prosecutors.
	Training	+	✓	+	+	ATF and the FBI do not have training on their policies to prohibit interfering with investigations into CIs, while the USMS does not have sufficient training in general.
	Foreign Operations	+	✓	✓	+	Although ATF and the USMS maintain that their CIs do not perform OIA abroad, their CIs are not prohibited from doing so and their policies lack coordination with DOJ on such matters.
	Deactivation	+	✓	✓	✓	ATF does not require delayed notification of deactivation to be documented in the CI file when the CI cannot be located.

 No Issues Identified
  Minor Issues Identified
  Revisions Required

Source: OIG analysis of component policies, procedures, forms, and training materials.

Considerations for CIs Performing OIA

The Department requires evaluation and approval of illegal activities conducted by CIs and directed by law enforcement officers commensurate with severity. Additionally, the Risk Assessment Memo requires law enforcement components to consider risk factors surrounding operations that potentially involve the “possession, transfer, or transportation of any dangerous commodity or item.” Although all components have OIA monitoring policies, we found that ATF, the DEA, and the USMS do not have complete policies to mitigate risks associated with CI operations involving dangerous commodities. Additionally, we found that ATF and USMS policies do not require written instructions to be provided to CIs before performing OIA in all required cases. Without appropriate policies, ATF, the DEA, and the USMS have not minimized the risks associated with OIA, such as the government’s active contribution to furthering criminal enterprises.

USMS Payment Process

While we found that the USMS has an electronic tracking system for approving and documenting CI payments, these payments are sent directly to Deputy U.S. Marshal bank accounts for withdrawal and payment to CIs. The AG Guidelines CI require establishing accounting and reconciliation procedures for CI payments but do not specify how the process must take place. As part of a robust accounting and reconciliation process, the AG Guidelines CI require law enforcement components to exercise sufficient controls and ensure risk mitigation throughout the disbursement process, such as submitting payments for advanced approval by management, ensuring at least two government personnel witness and disburse funds, collecting a receipt from the CI, and reconciling the amounts paid. However, the USMS’s current method increases operational security risks and does not adequately safeguard against fraud. USMS personnel told us that the USMS is working on a new process to pay CIs.

Recommendations

As a result of our audit, we provide five recommendations to ODAG, ATF, the DEA, the FBI, and the USMS.

We recommend that ODAG:

1. Evaluate the risks, enhance internal controls, and update its Confidential Informant guidance, as necessary, to address recent shifts in the law enforcement environment, emerging payment technology, differences between the AG Guidelines FBI CHS and AG Guidelines CI, and sources of information.

We recommend that ATF:

2. Enhance its policies and procedures to remedy identified deficiencies, including adding all suitability criteria in policy and forms, updating policy requirements for high-level CIRC review, documenting considerations made and outside approvals obtained for OIA conducted by CIs, incorporating all required training elements, and ensuring delayed notification of deactivation is documented in the CI file.

We recommend that the DEA:

3. Enhance its policies and procedures to remedy identified deficiencies, including considerations made when engaging parolees as CIs and documenting considerations made for OIA conducted by CIs.

We recommend that the FBI:

4. Enhance its policies and procedures to remedy identified deficiencies, including the clarification of certain disclosures to federal prosecutors and all required training elements.

We recommend that the USMS:

5. Enhance its policies and procedures to remedy identified deficiencies, including incorporating internal controls over its CI payment disbursement process that mitigates operational and misappropriation risks, documenting considerations made and outside approvals obtained for OIA conducted by CIs, and incorporating all required training elements.

APPENDIX 1: Audit Scope and Methodology

Scope and Methodology

To accomplish our objective, we reviewed the Attorney General's Guidelines Regarding the Use of Confidential Informants, the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources, and the "Baseline Risk Assessment and Mitigation Policies for Law Enforcement Operations in Criminal Matters" Memorandum (Risk Assessment Memo) issued by former Deputy Attorney General James M. Cole. These documents comprise the most recent Department-wide operational guidance for CIs. We then assessed CI policies and procedures implemented by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); and U.S. Marshals Service (USMS) to determine if these policies and procedures aligned with the appropriate Department guidance.⁷ In addition, we reviewed component training materials and forms and physically observed the components' CI-related information systems to ensure these systems also accounted for Department requirements. Further, we spoke with personnel from the Office of the Deputy Attorney General (ODAG), ATF, the DEA, the FBI, and the USMS. Throughout the audit, we obtained from responsible officials their feedback on our preliminary audit results; as appropriate, these views are reflected in our report.

Statement on Compliance with Generally Accepted Government Auditing Standards

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objective. We did not evaluate the internal controls of ODAG, ATF, the DEA, the FBI, and the USMS to provide assurance on their internal control structures as a whole. ODAG, ATF, the DEA, the FBI, and USMS management are responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the components' internal control structures as a whole, we offer this statement solely for the information and use of ODAG, ATF, the DEA, the FBI, and the USMS.

We reviewed the design of internal controls related to responding to risk, implementing policy, ensuring information systems achieve objectives, and communicating objectives internally. The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the audit objective, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

⁷ The Federal Bureau of Prisons (BOP) and DOJ's litigating offices and divisions, such as the United States Attorneys' Offices, do not use CIs in the same way as DOJ's law enforcement components. Instead, they obtain information from individuals who cooperate for non-monetary benefits. Therefore, we excluded the BOP and DOJ's litigating offices and divisions from the scope of our audit. Further, while the Office of the Inspector General (OIG) is authorized to use CIs, we excluded the OIG from the scope of our audit.

APPENDIX 2: Timeline of Office of the Inspector General Oversight Directly Related to Confidential Informants from Fiscal Year (FY) 2015 – Present

2024

December:

[A Review of the FBI’s Handling of its Confidential Human Sources and Intelligence Collection Efforts in the Lead up to the January 6, 2021 Electoral Certification.](#) **FBI**

In response to our recommendation, the FBI clearly defined in policy a mechanism for making a formal determination whether and what kind of a nationwide intelligence and CHS canvass is necessary and appropriate.

November:

[Notification of Concerns Identified in the DEA’s Transportation Interdiction Activities.](#) **DEA**

In November 2024, the Department issued guidance regarding DEA’s consensual encounters not related to existing investigations, and that the program is currently suspended while the Department considers further options.

August:

[Findings of Misconduct by a DEA Executive Assistant for Misuse of Position, Prohibited Association with a Former DEA Confidential Source, and Soliciting and Accepting Gifts from the Former DEA Confidential Source.](#) **DEA**

The OIG highlighted instances where a DEA employee did not follow policy.

2019

December:

[Review of Four FISA Applications and Other Aspects of the FBI’s Crossfire Hurricane Investigation.](#) **FBI**

As a result of recommendations, the FBI developed enhanced procedures to ensure that CHS information is documented in its CHS management system, Delta, including information generated from Headquarters-led investigations, substantive contacts with closed CHSs, derogatory information.

November:

[Audit of the FBI's Management of its Confidential Human Source Validation Processes.](#) **FBI**

As a result of recommendations, the FBI undertook a comprehensive review of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources, as well as internal FBI policy, processes, and procedures, to ensure that the FBI's CHS validation process was revised across the FBI. In December 2020, DOJ updated its guidelines to shift to a risk-based CHS validation process.

August:

[Findings of Misconduct by Two DEA Special Agents and a DEA Supervisory Special Agent for Violations of DEA's Confidential Source Policy.](#) **DEA**

The OIG highlighted instances where DEA Special Agents did not follow policy.

July:

[Findings of Misconduct by a DEA Group Supervisor for Actions related to a Confidential Source including Approving Payments to the Source without Proper Justification and Engaging in an Improper Personal Relationship; and by a DEA Assistant Special Agent in Charge for Failing to Properly Supervise the Group Supervisor.](#) **DEA**

The OIG highlighted instances where DEA Special Agents did not follow policy.

June:

[Audit of the Department of Justice's Use of Immigration Sponsorship Programs.](#) **ATF** **DEA** **FBI** **USMS**

As a result of the audit, the DEA and the FBI worked with the Department of Homeland Security to locate DOJ-sponsored individuals who had absconded. Additionally, all of the law enforcement components implemented methods to accurately and completely track all foreign national sponsorship information to help mitigate the risk of lapses in sponsorship or absconsion from DOJ control.

2018

April:

[Findings of Misconduct by an FBI Special Agent in Charge and Assistant Special Agent in Charge for Failing to Ensure Contact with a Known Drug Trafficker was Handled According to FBI Policy for Confidential Human Sources, and for Failing to Report and Preventing the Reporting of Misconduct Allegations.](#) **FBI**

The OIG highlighted instances where FBI Special Agents did not follow policy.

August:

[Findings of Misconduct by an FBI Special Agent for Receiving Gifts from a Former FBI Confidential Human Source, Using the Source After Deactivation, Protecting the Source and the Source's Illegal Business, Misusing FBI Assets for Personal Gain, Lack of Candor, and Computer Security Policy Violations.](#) **FBI**

The OIG highlighted instances where an FBI Special Agent did not follow policy.

2017

March:

[Public Summary of the Addendum to the Audit of the DEA's Management and Oversight of its Confidential Source Program.](#) **DEA**

[Audit of the ATF's Management and Oversight of Confidential Informants.](#) **ATF**

As a result of the audit, ATF implemented an improved CI recordkeeping system to maintain complete and reliable CI information. This updated system included a new feature to accurately and completely track payments and other benefits to CIs.

2016

September:

[Audit of the Drug Enforcement Administration's Management and Oversight of its Confidential Source Program.](#) **DEA**

As a result of the OIG's recommendations, the DEA refined and developed policies and practices to address risks associated with using confidential sources for interdiction operations and intelligence initiatives and overseeing sub-sources and established internal controls to improve the integrity of confidential source information and oversee payments to confidential sources.

2015

January:

[Findings Concerning the DEA's Use of Amtrak Employees as Paid Confidential Sources.](#) **DEA**

The OIG informed the public of instances in which Amtrak employees were used by DEA as confidential informants.

[Findings Concerning the DEA's Use of a Transportation Security Authority \(TSA\) Airport Security Screener as a Paid Confidential Source.](#) **DEA**

The OIG informed the public of instances in which a TSA employee was used by the DEA as a confidential informant.

July:

[Audit of the Drug Enforcement Administration's Confidential Source Policies and Oversight of Higher-Risk Confidential Sources](#) **DEA**

As a result of the OIG's recommendations, the DEA coordinated with the Criminal Division and Office of the Deputy Attorney General to update its policies to comply with the Attorney General Guidelines and enhance oversight of the DEA's use of long-term confidential sources and authorization of confidential sources to participate in otherwise illegal activities during operations.

APPENDIX 3: Office of the Deputy Attorney General's Response to the Draft Report



U.S. Department of Justice

Office of the Deputy Attorney General

950 Pennsylvania Ave., N.W.
RFK Main Justice Bldg.
Washington, D.C. 20530

MEMORANDUM

TO: Jason R. Malmstrom
Assistant Inspector General for Audit
Audit Division
Office of the Inspector General

FROM: Yamileth G. Davila
Associate Deputy Attorney General
Office of the Deputy Attorney General (ODAG)

DATE: October 23, 2026

SUBJECT: Department of Justice's Response to Draft Audit Report "Audit of the Department of Justice Components' Confidential Informant Policies"

Thank you for the opportunity to respond to the Office of the Inspector General (OIG) Report titled, "Audit of the Department of Justice Components' Confidential Informant (CI) Policies." OIG reviewed Attorney General guidance on the use of CIs and assessed whether each DOJ law enforcement component's policies complied with the appropriate Department guidance. OIG determined the Department needs to update guidance to consider the effects of recent Executive Orders, the prevalence of electronic payments, annual reporting requirements for CIs performing otherwise illegal activity (OIA), and management approval of high-level CIs. OIG made individual recommendations to law enforcement components. The following recommendation was made to the Department of Justice:

1. Evaluate the risks, enhance internal controls, and update its Confidential Informant guidance, as necessary, to address recent shifts in the law enforcement environment, emerging payment technology, differences between the AG Guidelines FBI CHS and AG Guidelines CI, and sources of information.

We concur with the recommendation. ODAG will work to address uniformity across the Department. ODAG will convene a working group consisting of representatives from the law enforcement components to update Department guidance. The working group will evaluate policy differences, current CI practices and risks, the use of sources of information, and internal controls within CI programs to ensure the Department's CI governance framework sufficiently addresses existing and emerging law enforcement topics. Specifically, ODAG will direct the Executive

Office for United States Attorneys (EOUSA), the Department of Justice Criminal Division (CRM), and law enforcement components—the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); and U.S. Marshals Service (USMS)—to collaboratively address these topics. The Acting Deputy Attorney General Trent McCotter will convene this working group within 120 days.

We appreciate OIG’s recommendations on this important topic, which has been and remains an important priority of the Department.

APPENDIX 4: Bureau of Alcohol, Tobacco, Firearms and Explosives' Response to the Draft Report



U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Assistant Director

Washington, DC 20226

www.atf.gov

701200: BTW
8310

September 18, 2026

MEMORANDUM TO: Assistant Director
Office of Professional Responsibility and Security Operations

FROM: Assistant Director
Office of Field Operations

SUBJECT: OIG Audit of the Department of Justice Components'
Confidential Informant Policies

This memorandum responds to the recommendations contained in the Office of Inspector General's (OIG) report titled "Audit of the Department of Justice Components' Confidential Informant Policies." We welcome OIG's constructive comments and appreciate the opportunity to respond.

Recommendation 1: Enhance its policies and procedures to remedy identified deficiencies, including adding all suitability criteria in policy and forms, updating policy requirements for high-level CIRC review, documenting considerations made and outside approvals obtained for OIA conducted by CIs, incorporating all required training elements, and ensuring delayed notification of deactivation is documented in the CI file.

ATF concurs with this recommendation. The Special Operations Division will update our policies, where appropriate, to align with the Attorney General (AG) guidelines. Specifically, we will augment orders, forms and training to capture all the individual component issues identified by OIG within the ATF confidential informant program. We expect to have this completed in FY 2027. ATF believes that, in practice, we are fully compliant with the AG Guidelines; however, we recognize that in some instances those practices are not currently memorialized in policy or articulated in a format reflective of the AG guidelines. ATF will endeavor to rectify our internal controls and the specified insufficiencies evaluated by OIG.

Please let me know if I can be of further assistance on this or any other matter.

**Brent
Beavers**

Digitally signed by Brent
Beavers
Date: 2026.09.18
12:07:04 -04:00

Brent Beavers

APPENDIX 5: Drug Enforcement Administration's Response to the Draft Report



U.S. Department of Justice
Drug Enforcement Administration
8701 Morrisette Drive
Springfield, Virginia 22152

www.dea.gov

MEMORANDUM

TO: Todd Anderson
Chicago Regional Audit Manager
Office of the Inspector General
U.S. Department of Justice

FROM: Eric Baldus
Deputy Chief Inspector
Office of Inspections

ERIC
BALDUS

Digitally signed by ERIC
BALDUS
Date: 2026.09.11
10:07:20 -04'00'

SUBJECT: DEA Response to the Office of Inspector General Draft Report titled, *Audit of the Department of Justice Components' Confidential Informant Policies*.

The Drug Enforcement Administration (DEA) has received the Department of Justice (DOJ) Office of the Inspector General's (OIG), Chicago Regional Audit Office Report titled, *Audit of the Department of Justice Components' Confidential Informant Policies*.

DEA appreciates OIG's work to address controls for emerging risks associated with the use of Confidential Informants (CIs) and to account for differences in component frameworks. DOJ has issued Department-wide operational guidance that establishes the internal control framework over CIs, undercover activity, and other law enforcement matters. This guidance includes the Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines CI), the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources (AG Guidelines FBI CHS), and the "Baseline Risk Assessment and Mitigation Policies for Law Enforcement Operations in Criminal Matters" Memorandum (Risk Assessment Memo) issued by former Deputy Attorney General James M. Cole. To decrease operational risks and safeguard taxpayer funds, DOJ's law enforcement components are required to operate within these guidelines by implementing internal controls that include formal policies, information systems, and training.

OIG has issued five recommendations in this review, recommendation 3 has been addressed to DEA.

DEA provides the response below to the report's DEA recommendation:

Recommendation 3: Enhance its policies and procedures to remedy identified deficiencies, including considerations made when engaging parolees as CIs and documenting considerations made for OIA conducted by CIs.

DEA Response

DEA concurs with the recommendation. DEA has initiated edits to its policy to clearly reflect the AG Guidelines and the former DAAG Cole Risk Assessment Memorandum, as recommended in OIG's recommendation. Further, along these lines, DEA has also considered OIG's concerns about the full application of the AG Guidelines towards Limited Use CSs and the use of DEA's risk assessment. DEA will update its policies and risk assessment forms for DEA leadership and Criminal Division's final review and approval.

Upon approval DEA will submit the updated policies for closure of this recommendation.

If you have any questions regarding this response, please contact Janice Swygert, Program Analyst, External Audit Liaison Team, at (571) 776-3119.

APPENDIX 6: Federal Bureau of Investigation's Response to the Draft Report



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 14, 2026

The Honorable Don R. Berthiaume
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Berthiaume:

The Federal Bureau of Investigation (FBI) appreciates the review your office conducted of our Confidential Human Source policies and the refinements suggested in your report entitled, *Audit of The Department of Justice Components' Confidential Informant Policies*.

The FBI is always looking to improve our policies to ensure they are not only consistent with Department policies and guidelines, but also instructive and user-friendly to our workforce. We look forward to working with the Office of the Inspector General to address the recommendation provided in the report.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Megan Hart", is positioned below the word "Sincerely,".

Megan Hart
Acting Assistant Director
Directorate of Intelligence
Federal Bureau of Investigation

UNCLASSIFIED

**The Federal Bureau of Investigation's Response to the Office of the Inspector General's
Audit of the Department of Justice Components' Confidential Human Source Policies**

OIG Recommendation: We recommend that the FBI enhance its policies and procedures to remedy identified deficiencies, including the clarification of certain disclosures to federal prosecutors and all required training elements.

FBI Response: The FBI concurs with the recommendation and will incorporate the suggested policy enhancements in our next round of policy edits. The policy updating process is already underway, so the FBI expects to be able to get the added and clarified policy language in place relatively soon, which will be early 2027.

UNCLASSIFIED

APPENDIX 7: United States Marshals Service's Response to the Draft Report



U.S. Department of Justice

United States Marshals Service

Office of Professional Responsibility

Washington, DC 20530-0001

September 23, 2026

MEMORANDUM TO: Jason M. Malmstrom
Assistant Inspector General
Office of the Inspector General

FROM: Ronald Carter
Assistant Director

RCarter Digitally signed by
RCarter
Date: 2026.09.23
11:08:49 -04'00'

SUBJECT: Response to Draft Audit Report: Audit of the Department of
Justice Components' Confidential Informant Policies

This is in response to correspondence from the Office of the Inspector General (OIG), requesting comment on the recommendation associated with the subject draft audit report. The United States Marshals Service (USMS) appreciates the opportunity to review the Report and concurs with the recommendations therein. Actions planned by the USMS with respect to OIG's recommendations are outlined in the attached response.

Should you have any questions or concerns regarding this response, please contact Krista Eck, External Audit Liaison, at 202-819-4371.

Attachments

cc: Todd Anderson
Regional Audit Manager
Office of the Inspector General

Louise Duhamel
Assistant Director, Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

John Kilgallon
Acting Chief of Staff
United States Marshals Service

**United States Marshals Service Response to the
Office of Inspector General Draft Report
Audit of the Department of Justice Components' Confidential Informant Policies**

Recommendation 5: Enhance policies and procedures to remedy identified deficiencies, including incorporating internal controls over its CI payment disbursement process that mitigates operational and misappropriation risks, documenting considerations made and outside approvals obtained for OIA conducted by CIs, and incorporating all required training elements.

USMS Response (Concur): The United States Marshals (USMS) is in the process of enhancing its policies and procedures to address the identified deficiencies and strengthen internal controls over the Confidential Informant (CI) Program. The USMS is currently working with a Global Financial Wire Transfer Company to finalize a payment system for Confidential Source (CS) and CI payments. Upon approval and implementation, the USMS will establish and document appropriate accounting and internal control procedures to ensure CS and CI payments are properly authorized, processed, documented, reconciled, and accounted for, with these procedures and associated internal controls incorporated into applicable USMS policy and guidance to mitigate operational and misappropriation risks. Additionally, the USMS will amend Form USM-340, *Confidential Informant Agreement*, to include a section addressing Otherwise Illegal Activity (OIA), and will revise USMS Policy Directive 8.14A, *Confidential Informants*, to provide guidance regarding OIA, including the documentation of considerations and required outside approvals. The USMS intends to strengthen training requirements under USMS Policy Directive 8.14A to ensure USMS investigators receive initial and follow-up training addressing the required elements associated with USMS investigator responsibilities for registered CIs. These policy, procedural, training, and internal control enhancements are intended to remedy the identified deficiencies and provide a consistent framework for the authorization, documentation, oversight, and administration of the CS and CI Programs, while addressing potential misappropriation risks.

APPENDIX 8: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

The Office of the Inspector General (OIG) provided a draft of this audit report to the Office of the Deputy Attorney General (ODAG), as well as to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); and the U.S. Marshals Service (USMS). ODAG's response is incorporated in Appendix 3 of this final report, while responses from ATF, the DEA, the FBI, and the USMS are incorporated in Appendices 4 through 7, respectively. In response to our audit report, all Department of Justice (DOJ) components concurred with our recommendations. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

Recommendation for ODAG:

1. **Evaluate the risks, enhance internal controls, and update its Confidential Informant (CI) guidance, as necessary, to address recent shifts in the law enforcement environment, emerging payment technology, differences between the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources (AG Guidelines FBI CHS) and Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines CI), and sources of information.**

Resolved. ODAG concurred with our recommendation. In its response, ODAG stated that it would address uniformity across the Department of Justice (DOJ) by convening a working group within 120 days to ensure DOJ's CI governance framework sufficiently addresses existing and emerging issues. ODAG stated that as part of this effort, the working group, comprised of appropriate DOJ component stakeholders, will evaluate CI policy differences, current CI practices and risks, use of sources of information, and internal controls within CI programs.

This recommendation can be closed when we receive evidence that the Department has evaluated the risks, enhanced internal controls, and updated its CI guidance, as necessary.

Recommendation for ATF:

2. **Enhance its policies and procedures to remedy identified deficiencies, including adding all suitability criteria in policy and forms, updating policy requirements for high-level Confidential Informant Review Committee (CIRC) review, documenting considerations made and outside approvals obtained for otherwise illegal activity (OIA) conducted by CIs, incorporating all required training elements, and ensuring delayed notification of deactivation is documented in the CI file.**

Resolved. ATF concurred with our recommendation. In its response, ATF stated that it plans to augment its orders, forms, and training to remedy identified deficiencies.

This recommendation can be closed when we receive evidence that ATF has updated its policies and incorporated all required training elements to remedy deficiencies identified in this report.

Recommendation for the DEA:

- 3. Enhance its policies and procedures to remedy identified deficiencies, including considerations made when engaging parolees as CIs and documenting considerations made for OIA conducted by CIs.**

Resolved. The DEA concurred with our recommendation. In its response, the DEA stated that it has initiated updates to its policy for deficiencies cited in this report.

This recommendation can be closed when we receive evidence that the DEA has updated its policies to remedy deficiencies identified in this report.

Recommendation for the FBI:

- 4. Enhance its policies and procedures to remedy identified deficiencies, including the clarification of certain disclosures to federal prosecutors and all required training elements.**

Resolved. The FBI concurred with our recommendation. In its response, the FBI stated that it has initiated updates to its policies for deficiencies cited in this report.

This recommendation can be closed when we receive evidence that the FBI has clarified its policies and incorporated all required training elements to remedy deficiencies identified in this report.

Recommendation for the USMS:

- 5. Enhance its policies and procedures to remedy identified deficiencies, including incorporating internal controls over its CI payment disbursement process that mitigates operational and misappropriation risks, documenting considerations made and outside approvals obtained for OIA conducted by CIs, and incorporating all required training elements.**

Resolved. The USMS concurred with our recommendation. In its response, the USMS stated that it is working to update policies, procedures, and forms to remedy identified deficiencies. The USMS further stated that it is addressing the payment process with a third party and will update its policies after finalizing the new process. Finally, the USMS stated that it will strengthen its training to align with policy enhancements.

This recommendation can be closed when we receive evidence that the USMS has updated its policies and incorporated all required training elements to remedy deficiencies identified in this report.