



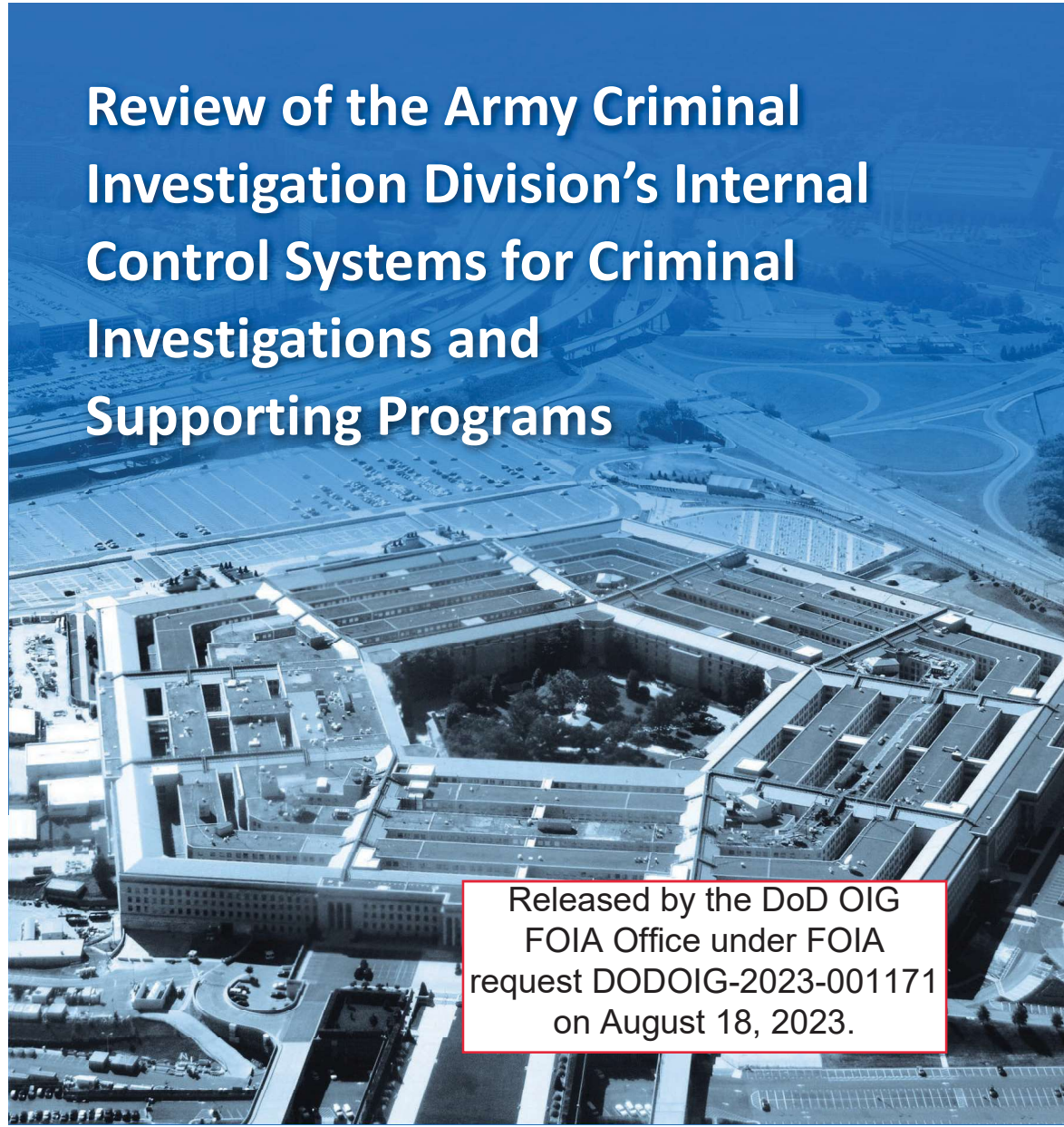
INSPECTOR GENERAL

U.S. Department of Defense

JANUARY 23, 2023



Review of the Army Criminal Investigation Division's Internal Control Systems for Criminal Investigations and Supporting Programs



Released by the DoD OIG
FOIA Office under FOIA
request DODOIG-2023-001171
on August 18, 2023.

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE





OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 23, 2023

MEMORANDUM FOR DIRECTOR, U.S. ARMY CRIMINAL INVESTIGATIONS DIVISION

SUBJECT: Review of the Army Criminal Investigation Division's Internal Control Systems
for Criminal Investigations and Supporting Programs

This final report provides the results of the DoD Office of Inspector General's review. We provided a draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

The CID Chief of Staff agreed to address all the recommendations presented in the report; therefore, we consider the recommendations resolved and open. As described in the Army CID Comments and Our Response section of this report, we will close the recommendations when you provide us documentation showing that you completed all agreed-upon actions to implement the recommendations. Therefore, please provide us your response within 90 days concerning specific actions in process or completed on the recommendations. Send your response to DODOIG (b) (6) @dodig.mil.

If you have any questions, please contact DODOIG (b) (6) at DODOIG (b) (6), (DSN DODOIG (b) (6)).

A handwritten signature in black ink, appearing to read "Randolph R. Stone", is located below the text.

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, engineering, and Oversight

Contents

Executive Summary

Objectives	1
Background	2

Observations – Objective 1

Army CID Inspector General and Manager’s Internal Control Program Review	3
Recommendation	3

Observations – Objective 2

Investigative Case File Review	4
--------------------------------------	---

Observations – Objective 3

Support Programs Review	5
.0015 Contingency Limitations Fund	7
ARMY CID (b) (7)(E)	7
Special Victim Investigations Team Operations Program	8
Evidence Program	9
ARMY CID (b) (7)(E)	10
Weapons Program	10
Training Program	11
Recommendation	12
Army CID Comments	13
Our Response	13

Appendix A - Scope and Methodology

Objective 1. Inspector General and Manager’s Internal Control Program	14
Objective 2. Investigative Case File Review	15
Objective 3. Support Programs Assessment	16

Management Comments

Army CID Comments	18
-------------------------	----

Acronyms and Abbreviations	19
----------------------------------	----

Executive Summary

We determined that the Army Criminal Investigation Division (CID) generally complied with DoD, Service, and Army CID policies and procedures, as well as with Council of the Inspectors General on Integrity and Efficiency “Quality Standards for Investigations,” November 15, 2011, and the “Quality Standards for Inspection and Review,” published in January 2012, and revised in December 2020.

However, we determined the Army CID lacked internal controls to ensure that Army CID Inspector General (IG) inspections contained specific performance standards, recommendations, and follow-up procedures to operate effectively. Furthermore, we found areas of noncompliance with required policy updates and other administrative requirements. We determined these observations did not adversely affect the Army CID’s ability to respond to and investigate allegations of criminal incidents. Lastly, we identified areas for improvement for increased efficiency and effectiveness, which we discuss later in this report.

We made one recommendation to improve CID policies and procedures for the internal controls of the CID IG inspection process, and 10 recommendations to improve policies and procedures for investigative support programs.

Objectives

The objectives of this review were to:

1. Determine the extent to which Army CID internal controls and inspections were suitably designed and operating efficiently and effectively, to provide reasonable assurance that its personnel were complying with investigative standards, as required by DoD, Service, and Army CID policy, to ensure high quality and timely criminal investigations.
2. Determine the extent to which Army CID personnel responded to and investigated allegations of criminal incidents, as required by DoD, Service, and Army CID policy.
3. Determine the extent to which Army CID investigative support programs provided efficient and effective support to criminal investigations.

Background

Within the Army, the Army CID “exercises command authority, direction, and control of Army criminal investigative activities worldwide.”¹ The Army CID IG has the responsibility and the regulatory requirement to oversee the efficiency, effectiveness, and integrity of Army CID operations and personnel, including that the Army CID complies with professional investigative standards.²

The DoD Office of Inspector General (DoD OIG) conducted a review of Army CID operations and programs in accordance with our oversight authority to monitor and evaluate the Military Criminal Investigative Organizations’ (MCIOs) programs.³

We reviewed the operations, policies, and procedures of the Army CID from January 1, 2018, to December 31, 2021. The scope for this review is in two parts.

- In November 2020, we chose for review a sample of investigative case files that met specific criteria from investigations conducted from January 1, 2018, to December 31, 2019.⁴
- We conducted site visits to review support programs and operations conducted from January 1, 2019, to December 31, 2021.

¹ AR 195-2, “Criminal Investigation Activities,” August 21, 2020.

² AR 20-1, “Inspector General Activities and Procedures,” July 3, 2012, outlines the role of Army Inspector General personnel and Criminal Investigation Division Regulation 1-201 outlines the CID Inspector General responsibilities.

³ DoD Instruction 5505.03, “Initiation of Investigations by Defense Criminal Investigative Organizations,” March 24, 2011, (Incorporating Change 2, February 13, 2017), defines the MCIOs as the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, and Air Force Office of Special Investigations.

⁴ The Army CID provided an initial sample of 11,812 criminal investigations that were initiated on or after January 1, 2018, and closed (completed and adjudicated) on or before December 31, 2019. From the closed criminal investigations listing, we excluded investigations that the CID worked jointly with another law enforcement agency. We also excluded cases with a low rate of occurrence and with minimal investigative effort, for example, positive urinalysis narcotics cases and providing a false statement. We determined that 4,765 criminal investigations met our criteria for review. We evaluated 190 CID criminal investigations, including 44 Crimes against Property, 47 Drug Crimes, 49 Crimes against Persons, and 50 Sex Crimes.

Observations – Objective 1

Army CID Inspector General and Manager's Internal Control Program Review

Objective 1. Determine the extent to which Army CID internal controls and inspections were suitably designed, and operating efficiently and effectively, to provide reasonable assurance that its personnel are complying with investigative standards, as required by DoD, Service and Army CID policy, to ensure high quality and timely criminal investigations.

In general, the Army CID complied with internal controls required by DoD, Service, and Army CID policies, with exceptions noted in this report. Criminal Investigation Division Regulation (CIDR) 1-201 directs that, as part of the Organizational Inspection Program (OIP), the Army CID IG will inspect battalions and specialty CID field elements, such as the Field Investigative Unit and Protective Services Battalion, every 2 years.⁵ As part of the OIP, Army CID IG is required to produce a report that addresses “findings, observations, root causes, and recommendations.” CIDR 1-201 states, “Recommendations are only effective if the commander assigns responsibility to individuals to ensure corrective actions identified during all inspections are implemented and completed properly.” However, interviews of Army CID personnel who administer the OIP process at the Headquarters (HQ), group, and battalion levels disclosed that group and battalion inspection personnel do not always track open recommendations and ensure corrective action for the group and battalion inspection findings. As a result, the Army CID IG does not consistently follow up on open recommendations to ensure recommendations are implemented and completed properly and, further, cannot validate that Army CID units are complying with DoD, Service, and Army CID policies.

Recommendation

- 1. We recommend that the Director of the U.S. Army Criminal Investigation Division designate an office of primary responsibility at headquarters and subordinate commands for all Army Criminal Investigation Division inspection programs, with responsibility for establishing procedures for tracking and following up on open recommendations.**

⁵ CIDR 1-201, “Organizational Inspection Program,” March 5, 2019, paragraph 4-3(d).

Observations – Objective 2

Investigative Case File Review

Objective 2. Determine the extent to which Army CID personnel responded to and investigated allegations of criminal incidents, as required by DoD, Service, and Army CID policy.

Our review of a sample of 190 of 4,765 criminal investigations conducted between January 1, 2018, and December 31, 2019, determined that the Army CID generally conducted criminal investigations in an independent and thorough manner, correctly documented investigative activities, ensured legal sufficiency, and maintained complete and accurate criminal investigations-related data.

Observations – Objective 3

Support Programs Review

Objective 3. Determine the extent to which Army CID investigative support programs provided efficient and effective support to criminal investigations.

We determined that the Army CID:

- Managed the .0015 Funds Contingency Limitation Program in accordance with Service and Army CID regulations, with significant oversight from Army CID leadership and the U.S. Army Financial Management Command.⁶ Army CID units correctly documented funds, cash counts, and physical security measures and correctly retained supporting expenditure receipts. However, Army Regulation (AR) 195-4 does not specifically address tipping for meal reimbursements. The lack of clear policy on tipping results in confusion and inconsistent reimbursement.
- ARMY CID (b) (7)(E) [REDACTED]
- Organized the Special Victims Investigations teams in accordance with Army CID regulations and properly trained and certified Army CID agents who conduct special victim investigations.
- Managed the Evidence Program in accordance with AR 195-4 and with continuous oversight from Army CID leadership.⁸ The Army CID developed standardized evidence custodian training, but did not execute that training centrally, resulting in inconsistent application of the program. Additionally, the Army CID does not have internal control procedures to verify the disposal of evidence.

⁶ .0015 Contingency Limitation funds are appropriated funds used for emergency and unusual expenditures where it would not be practical to use a Government purchase card, travel card, or other traditional method of payment for expenses incurred while conducting investigations, gathering criminal intelligence, crime prevention, conducting protective services mission, and purchasing equipment and supplies under certain circumstances and with specific limitations, as defined in CIDR 195-4.

Army Regulation (AR) 195-4, "Use of Contingency Limitation .0015 Funds for Criminal Investigative Activities," March 30, 2020.

CIDR 195-1, "Criminal Investigation Operational Procedures," January 4, 2016.

⁷ CIDR 195-1 [REDACTED]

[REDACTED] CIDR 195-1 [REDACTED]

⁸ AR 195-5, "Evidence Procedures," August 25, 2019.

- ARMY CID (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].
- Managed the Weapons Program in accordance with Army CID regulations, with general oversight from Army CID leadership. However, the program is not a consolidated weapons program with program managers who attended the Federal Law Enforcement Training Center's Firearms Instructor Course or an equivalent course.⁹
- Does not have internal control procedures to verify that Army CID agents annually completed the Lautenberg Amendment Certifications, in accordance with Army CID regulations.
- Does not consistently equip assigned Drug Suppression Team (DST) personnel with weapons, as required by CIDR 195-1 and CIDR 190-14. Additionally, DST personnel use their personal cell phones for official duties, which could potentially place DST personnel at risk from subjects of criminal investigations. Furthermore, DoD Instructions 5015.02 and 8170.01 mandate the preservation of text messages as official records under specific circumstances.¹⁰
- Did not manage the Command Training Program for annual and ancillary training in accordance with Army regulation.¹¹ The Army established internal controls through the Digital Training Management System (DTMS). However, Army CID personnel responsible for tracking training are not familiar with DTMS and are not keeping DTMS records up to date.

We identified the following areas for improvement, or increased efficiency and effectiveness, during our site visits to Army CID components at two Army CID group headquarters, three Army CID battalion offices, and four Army CID installation offices.¹²

⁹ CIDR 190-14, "Carrying, Using, Safeguarding, and Qualifying with Weapons," June 19, 2018 (Updated April 1, 2020); "Lautenberg" is common law enforcement terminology for an amendment to the Gun Control Act of 1968 (18 U.S.C § 922 [g] [19]) implemented in DoD Directive 5210.56, "Arming and Use of Force," that requires law enforcement agencies to certify that personnel issued Government-owned firearms have not been convicted of a domestic violence offense.

¹⁰ DoD Instruction 5015.02, "Records Management Program," February 24, 2015, Incorporating Change 1, August 17, 2017 DoD Instruction 8170.01, "Online Information Management and Electronic Messaging" January 2, 2019, Incorporating Change 1, August 24, 2019.

¹¹ AR 350-1, "Army Training and Leader Development," December 10, 2017.

¹² CID groups are subordinate headquarters comprising multiple battalions and specialty units that are responsible for criminal investigation activities with an Army interest for the assigned geographic area.

.0015 Contingency Limitations Fund

We identified areas for improvement related to the .0015 Contingency Limitations Fund Program. AR 195-4 does not address tipping for meal reimbursements for special agents conducting source operations. At one location, an Army CID special agent told us that AR 195-4 does not explicitly allow tipping for meal reimbursements purchased during source operations, which leads to confusion as to whether tips are authorized. Tipping for food service is a common practice in the United States. Failing to abide by common practices while conducting source operations attracts unwarranted attention to the source and source handler, possibly resulting in compromise of the source or the source operation. Furthermore, tipping without authorized reimbursement could potentially result in the special agent falsifying a claim in order to recover personal funds expended during the source operation.

At one battalion we visited, the .0015 fund manager told us that special agents can claim reimbursement for tipping. Additionally, the .0015 fund manager said that the special agent must detail the expense in the Case Activity Summary (CAS), but not on the Department of the Army (DA) Form 5070.¹³ However, we found no requirements in AR 195-4 that addressed documenting tipping in the CAS. The lack of clear policy on tipping by special agents conducting source operations for meal reimbursement results in confusion and inconsistent reimbursement.

ARMY CID (b) (7)(E)



ARMY CID (b) (7)(E)



¹³ AR 195-4 requires CID special agents to prepare a DA Form 5070 for reimbursements and submit it to the paying agent within 5 days of the expenditure of .0015 funds.

ARMY CID (b) (7)(E)

[Redacted text block]

[Redacted text block]

Special Victim Investigations Team Operations Program

We determined that the Army CID does not track sexual assault investigations training; therefore, the Army CID does not meet the intent of the CIDR 195-1 requirement to ensure that Special Victim Investigators have yearly sexual assault refresher training. Specifically, we found that neither the 3rd or 6th CID Group tracks how many Special Victim Investigators have completed initial or advanced sex crimes investigations training to receive the basic or senior Special Victim Investigators status. The Army CID also does not track refresher sexual assault investigations training. We determined that the Army CID group training readiness assessments of trained personnel only provide current training levels of certifying

14 [Redacted footnote text]

sexual assault investigation courses at the battalion level. Additionally, the Army CID does not track the assignment of personnel to ensure the field units have sufficient fully trained personnel to conduct sexual assault investigations.

Evidence Program

The Army CID training academy does not teach a standardized evidence custodian course. Instead, Army CID leadership provides new evidence custodians with localized training at the unit where the evidence custodian is assigned. The Army CID established an evidence training program called Evidence Management Certification Course (EMC2) for localized training. The EMC2 training program consists of viewing a PowerPoint presentation, conducting practice exercises, reading policy narrative, and discussing lessons learned with the trainer. The lack of standardized training organized by a primary office of responsibility could result in inconsistent application of evidence procedures throughout the Army CID.

At one detachment, we reviewed a sample of inactive DA Forms 4137, Evidence/Property Custody Document, and determined that the evidence custodian

ARMY CID (b) (7)(E)

Retaining excess items in evidence storage can lead to improper storage.

Additionally, at two detachments, the evidence custodian told us that they were required to dispose of the same amount of evidence that the unit seized each month. AR 195-5 establishes the guidelines for the disposition of evidence when the item is determined to have no evidentiary value, or the trial counsel determines that retention of the evidence is no longer required. There is no regulatory guidance allowing for the arbitrary disposal of evidence due to space constraints or for the convenience of the evidence custodian. Encouraging evidence custodians to dispose of evidence risks the premature disposal of evidence that could later prove beneficial to the adjudication of the criminal allegation. Furthermore, this practice may violate Section 586 of Public Law 112-81, which requires that “the length of time physical evidence and forensic evidence must be retained shall be not less than five years” when the evidence is related to a sexual assault.¹⁶

¹⁵ CIDR 195-1, October 1, 2020, Appendix D, “Criminal Investigation Standards,” undated.

¹⁶ Public Law 112-81, “National Defense Authorization Act for Fiscal Year 2012,” Section 586, “Department of Defense policy and procedures on retention and access to evidence and records relating to sexual assaults involving members of the Armed Forces,” December 31, 2011.

ARMY CID (b) (7)(E)

ARMY CID (b) (7)(E)

At one location, we identified that DST personnel use their personal cell phones for official duties. ARMY CID (b) (7)(E)

According to DST personnel, their battalion leadership denied their request for government cell phones because the DST personnel are MPs and not Army CID special agents. The use of personal cell phones to conduct official business could potentially place DST personnel at risk. Criminal targets of the investigations conducting an internet search of phone numbers can obtain the home address of DST personnel. All Army CID personnel, including the DST, should use government cell phones for official business to reduce the risk of compromising operations and personnel safety.

Weapons Program

We visited nine locations and unit leadership at each location could not provide Department of Defense (DD) Forms 2760 for all personnel assigned a firearm, as required by CIDR 190-14.¹⁷ As a result, Army CID leadership cannot determine whether personnel are qualified to possess a firearm or are prohibited from possessing a firearm. At one location, the armorer told us that they were unaware of the requirement to complete the form annually. CIDR 190-14 requires annual training on the Lautenberg Amendment and completion of DD Form 2760 to certify compliance. Furthermore, the Army CID has no overarching weapons program or HQ weapons program manager. The lack of an Army CID weapons program manager could result in less accountability and inconsistent application of policy.

¹⁷ DD Form 2760, "Qualification to Possess Firearms or Ammunition," is a form completed by agents to determine whether the agent was convicted of a crime of domestic violence, which would disqualify the agent from possessing a firearm. Specifically, an agent convicted of domestic violence is not be permitted to ship, transport, possess, or receive Government-issued or private firearms or ammunition. In addition the form can be used to determine whether the DoD should reassign, reclassify, detail, or take another administrative action for the agent.

ARMY CID (b) (7)(E)

At one location, two Army CID members told us that 16 DST members, comprised mostly of MPs, rotate the use of two CID weapons. The DST team chief at this location told us that, although

, the MOU did not address the transfer of weapons for those MPs attached to the Army CID. As a result, those DST members do not necessarily train and qualify on the duty weapon they carry. The MOU in effect during our site visit did not address MP weapons, but the Army CID unit was in the process of updating the MOU. In the event of an officer-involved shooting, the Army CID would be responsible for DST personnel carrying and using a weapon without proper training or qualification.

CIDR 190-14 mandates that Army CID field element Special Agents-in-Charge and Resident Agents-in-Charge will, “ensure all Army CID personnel have qualified with their assigned weapon... and, at a minimum, have fired for familiarization with any other authorized weapon prior to use.” We determined that DST personnel do not always train and qualify on the weapon they carry when on duty.

Training Program

We determined that training personnel did not always use the Digital Training Management System (DTMS) as a training management tool. We found that unit training personnel used a shared drive and a Microsoft Excel document to track training status, rather than DTMS, at all eight locations we visited.

At four detachments, we found that the detachment sergeants could not show us complete training records in DTMS for all assigned personnel. Furthermore, the detachment sergeants could not produce complete training records stored outside of DTMS for all assigned personnel.¹⁹ None of the detachment sergeants were able to produce documentation to validate that agents completed all required training. The detachment sergeants attributed their inability to produce the training records, as required by AR 350-1 and AR 220-1, to a variety of issues, including inexperience, lack of awareness, and limitations from the coronavirus disease–2019 (COVID-19) pandemic.²⁰

¹⁸ CIDR 195-1, Appendix J, “Guide for Preparing MOU for DST,” October 1, 2020.

¹⁹ Examples of the training include Combating Trafficking in Persons, Flying while Armed, Information Assurance, and other ancillary and annual training. This training is required by for military and civilian special agents assigned to Army CID.

²⁰ AR 220-1, “Army Unit Status Reporting and Force Registration – Consolidated Policies,” April 15, 2010.

AR 350-1 states that the Army Training Management System consists of the Army Training Network and DTMS and “is the Army’s primary tool that provides access to training strategies.” AR 220-1 prescribes DTMS as “the system that will be used to track and schedule training and provide summary reports to assist in determining individual and collective skill proficiency for assessing unit overall training.” AR 350-1 specifies, “DTMS is the required automated system to use to assist the commander/trainer in planning, resourcing, and tracking individual and collective unit training tasks,” and mandates using DTMS for managing unit training. In addition to DTMS, AR 350-1 suggests that supervisors “maintain records of employee training during the duty day.” On March 8, 2019, the Army CID commanding general released a memorandum that directed DTMS use, specified DTMS as the only automated system of management for training records in the Army, and directed units to ensure DTMS contained all training data on Soldier readiness for Army CID personnel.

Recommendation

- 2. We recommend that the Director of the U.S. Army Criminal Investigation Division:**
 - a. Revise the .0015 contingency limitation funds policy to add specific guidance on the procedure for payment of and documentation of tips paid during law enforcement activities.**
 - b. Develop policy to establish training and operational guidance for source handler training, specifically addressing the tactics, techniques, and procedures for source recruitment, tasking, and termination.**
 - c. Develop and implement a source management program at headquarters, led and managed by a program manager with experience in law enforcement and in conducting and overseeing source operations including source handler training, specifically addressing the tactics, techniques, and procedures for source recruitment, tasking, and termination.**
 - d. Develop and implement a plan for ensuring special agents assigned to Special Victims Investigations complete team training, as required by Criminal Investigation Division Regulation 195-1.**
 - e. Develop internal control procedures to validate that Army Criminal Investigation Division units are complying with existing requirements in Criminal Investigation Division Regulation 195-1 regarding the disposition of evidence.**
 - f. Designate an office of primary responsibility for standardizing the Evidence Custodian Management Certification Training.**

- g. Develop and implement an undercover operations program at headquarters, led and managed by a program manager with experience in law enforcement and in conducting and overseeing undercover operations.**
- h. Develop and implement Drug Suppression Team memorandums of understanding that fully identify equipment requirements, including weapons and cellular phones, for all assigned members, including members tasked from local military police units.**
- i. Develop and implement internal control procedures for the Army Criminal Investigation Division Inspector General to validate compliance with Criminal Investigation Division Regulation 190-14 to complete Lautenberg certifications.**
- j. Develop and implement internal control procedures for the validation of training in the Digital Training Management System.**

Army CID Comments

The CID Chief of Staff, responding on behalf of the CID Director, agreed with all of our recommendations. The Chief of Staff told us in his response memorandum that CID is undergoing a complete transformation of its investigative operations and support programs. The Chief of Staff told us that “policy, oversight, management and implementation of internal controls in the areas” including .0015 contingency funds, agent training, source operations, evidence management, drug suppression operations and compliance with Lautenberg certifications will be implemented within 6 months. The Chief of Staff agreed to provide copies of new policies and management controls when they are complete.

Our Response

The comments from the Army CID Chief of Staff addressed our recommendations. Therefore, the 11 recommendations are resolved, but will remain open. We will close the recommendations when we validate that corrective actions were implemented.

Appendix A - Scope and Methodology

We conducted this review from February 2021 through October 2022 in accordance with the “Quality Standards for Inspection and Review,” published in January 2012, and revised in December 2020, by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the review to ensure that objectives are met and that we perform the review to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

The scope for this review covered two time periods. We reviewed a sample of investigative case files in which the Army CID was the lead investigative agency for criminal investigations conducted from January 1, 2018, to December 31, 2019. We also reviewed the operations, policies, and procedures of the Army CID from January 1, 2018, to December 31, 2021.

Objective 1. Inspector General and Manager’s Internal Control Program

We conducted this review using guidelines from the Council of the Inspectors General on Integrity and Efficiency, and DoD, Service, and Army CID policies. We determined whether the Army CID Director complied with DoD, Service, and Army CID policies; whether Army CID internal controls are in place, suitably designed, and operating effectively; and whether there were areas for improvement.

We selected Army CID groups, battalions, and field offices for review based on the following criteria, which resulted in selecting nine sites to visit:

- number, size, and geographic dispersion of field offices;
- number, type, and significance of reports issued by location;
- degree of battalion control over field locations;
- results of prior internal inspection reports; and
- need to verify the results of internal inspection reports.

We developed site visit guides to assess the detachments’ internal management procedures and internal controls. Additionally, we reviewed training records to determine whether investigators maintained their investigative and law enforcement skills and met with various levels of Army CID professional staff to assess their compliance with relevant quality control policies and procedures.

In response to our October 29, 2020, data call memorandum, the Army CID IG provided Army CID directives, instructions, regulations, manuals, pamphlets, standard operating procedures, internal implementing-type memorandums, and other policy documents, along with effective dates and record retention requirements applicable to investigative and program oversight compliance and inspection programs. Using that information, we developed meeting discussion guides to support our objectives. We reviewed the Army CID inspection report findings and recommendations to determine Army CID field units' responses to the Army CID IG's findings and recommendations and to assess compliance with Army CID policy. We also conducted investigative and administrative program reviews at Army CID headquarters and met with Army CID subject matter experts and program managers.

Objective 2. Investigative Case File Review

We requested that the Army CID provide a list of all criminal investigations that were initiated on or after January 1, 2018, and closed (completed and adjudicated) on or before December 31, 2019.²¹ We excluded investigations that the Army CID worked jointly with another law enforcement agency where the Army CID was not the lead agency to allow for a more accurate assessment of the Army CID's performance in these investigations. Following discussion with the Army CID IG representatives about Army CID investigative case file categories, we divided the sample of criminal investigations into the National Incident Based Reporting System's categories and then sub-divided the narcotic cases from property crimes.²²

The DoD OIG Quantitative Methods Division (QMD) reviewed the list of 4,765 criminal investigations and identified a stratified random sample of 190 investigative case files to evaluate, based on a desired level of reliability. Specifically, we requested a sample from the population using a 90-percent confidence level, 95-percent probability of occurrence, and a 5-percent precision level. The Army CID provided the 190 specified investigative case files for review.

Our investigative case file review of the sample of 190 case files addressed the investigative steps that are essential to completing a thorough criminal investigation that complies with applicable DoD, Service, and Army CID policies in effect at the time the investigation was conducted. We reviewed the Army

²¹ We used January 2018 to December 2019 as the scope for the investigative case file review to capture the largest number of completed and adjudicated cases that had been digitized and uploaded to the CID system. "Completed and Adjudicated" means that CID has completed investigative activity, referred the investigation for command action, and received a completed report of command action or declination.

²² National Incident-Based Reporting System categories are Crimes against Persons, Crimes against Property, and Crimes against Society. The CID transmits case data to the Defense Incident Based Reporting System to populate case type categories in the National Incident-Based Reporting System.

CID's investigative policy to assess the extent to which the policy addressed the required investigative activity in response to a criminal allegation. The core of the investigative case file review protocol contained subsections that addressed investigative processes specific to the case type. We collectively reviewed four cases at the start of the project to help in the normalization of the review process and input the review information into a case assessment database. This process was designed to test the functionality of the case review checklist as well as form a baseline for the review team and set a standard for a consistent process among the evaluators.

In conducting the review of the sample, we assessed the investigative files for investigative sufficiency to identify deficiencies that affected the outcome of the investigation and deficiencies that did not meet DoD, Service or Army CID policy requirements. We also noted technically compliant investigative steps that could have been enhanced by further effort, more detailed documentation, or timely actions by the investigator. We categorized the results of the review of investigative files into three groups: "meets standards," "meets standards with comments," and "does not meet standards."

At the conclusion of the case review, we analyzed the data collected and stored in our case assessment database by developing Microsoft Access queries to identify investigative tasks and steps that were not completed. The queries revealed the investigative tasks or steps involved with each deficiency and the number of instances of each.

Objective 3. Support Programs Assessment

Based on our review of Army CID operations, we selected four investigative support programs and five non-investigative support programs to evaluate. Specifically, we selected the following investigative support programs: Evidence collection and handling Source Management, Special Victim Investigations Team Operations, and Undercover Operations because these programs directly support Army CID criminal investigations. We also selected the following non-investigative support programs: .0015 Contingency Limitation Funds, Training, and Weapons. We selected these non-investigative support programs because they help the special agents' mission execution by providing resources for personal safety, a mechanism to pay for unexpected official duties expenses, and tools to support agents' mental health.

We visited the same nine sites identified in objective 1 to determine how the investigative support programs were executed at the various subordinate unit levels. We selected these locations after coordination with subject matter experts

at HQ Army CID to determine which Army CID locations would provide our team with the best opportunity to review the selected programs. In addition, we selected these locations because of the large size of the unit and the broad missions.

Management Comments

Army CID Comments



DEPARTMENT OF THE ARMY
U. S. ARMY CRIMINAL INVESTIGATION DIVISION
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

CIOP-ZC (195)

9 January 2023

MEMORANDUM FOR Office of Inspector General (Deputy Inspector General for Policy and Oversight), Department of Defense, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Review of the Army Criminal Investigation Division's Internal Control Systems for Criminal Investigations and Supporting Programs (Project No. D2021-DEV0SV-0091.000)

1. Reference your report, dated 8 Dec 22, subject as above.
2. Thank you for the opportunity to provide comments to the report. I acknowledge your detailed review of the U.S. Army Criminal Investigation Command (CID) policies and procedures associated with internal control systems.
3. I reviewed the report and recommendations and concur with the all the recommendations. As you are aware, CID is undergoing a complete transformation of its investigative operations and support programs.
 - a. With CID's recent appointment as the proponent agency for many Army Regulations (AR) regarding investigations, to include .0015 contingency funds, revising AR 195-4 to add specific guidance regarding tips should be accomplished within the next six months. A copy of the revised policy will be provided to you when complete.
 - b. It is expected that policy, oversight, management and implementation of internal controls in the areas of agent training, source operations, evidence management, drug suppression operations, and compliance with Lautenberg certifications will all be implemented within the next six months. As these matters are completed, copies of the policies and management controls will be provided to you when complete.
4. The point of contact is [REDACTED]

ARMY CID (b) (6) and (b) (7)(C)

Chief of Staff

Acronyms and Abbreviations

AR Army Regulation

CID United States Army Criminal Investigation Division

CIDR CID Regulation

DST Drug Suppression Team

MOU Memorandum of Understanding

ARMY CID (b) (7)(E)

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

**For more information about DoD OIG
reports or activities, please contact us:**

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline





DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

