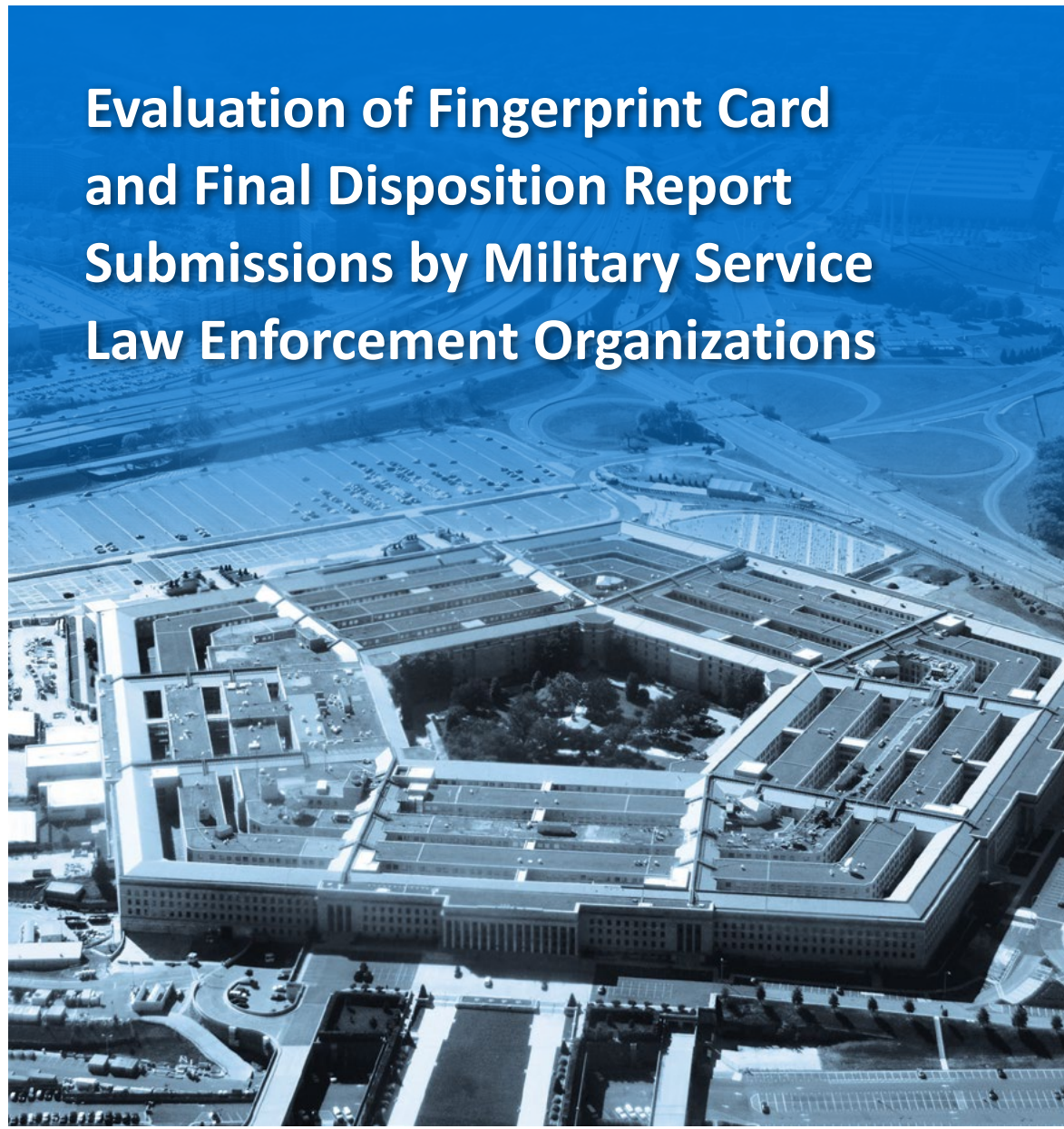




INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 4, 2017



Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste, & Abuse

HOTLINE

Department of Defense

dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.



Results in Brief

Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations

December 4, 2017

Objective

The objective of our evaluation was to determine whether all Military Services Law Enforcement Organizations (LEOs) had submitted fingerprint cards and final disposition reports for Military Service members convicted by court-martial of qualifying offenses, as required by DoD instruction. We reviewed these submissions for the period from January 1, 2015, to December 31, 2016.

Findings

For this time-period, we identified a total of 2,502 convicted offenders from the Military Services whose fingerprint cards and final disposition reports were required to be submitted to the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) for inclusion in the FBI's Next Generation Identification (NGI) database.

Findings (cont'd)

The FBI NGI database is a national computerized system for storing, comparing, and exchanging fingerprint data and criminal history information for law enforcement purposes.

The FBI NGI's primary function is to provide the FBI a fully automated fingerprint identification and criminal history reporting system. The failure to populate the NGI with all the required fingerprint records can allow someone to purchase a weapon who should not, hinder criminal investigations, and potentially impact law enforcement and national security interests.

We determined that the Military Services did not consistently submit fingerprint cards and final disposition reports as required. Overall, of the 2,502 fingerprint cards required to be submitted, 601 (24 percent) were not submitted. Of the 2,502 final disposition reports required to be submitted, 780 (31 percent) were not submitted.

The results differed by Service. As shown in the following table, the Army, Navy, and Marine Corps failed to submit many such fingerprint cards and final disposition reports, as required. The Air Force performed better, but still had missing fingerprint cards and final disposition reports.

Service	LEO	Convictions	Fingerprint Card Submissions				Final Disposition Report			
			Submitted	Not Submitted	Submitted	Not Submitted				
Army		948	686	72%	262	28%	563	59%	385	41%
USACIDC		768	609	79%	159	21%	504	66%	264	34%
Army MP		180	77	43%	103	57%	59	33%	121	67%
Navy		682	485	71%	197	29%	439	64%	243	36%
NCIS		631	472	75%	159	25%	428	68%	203	32%
Navy SF		51	13	25%	38	75%	11	22%	40	78%
Air Force		743	638	86%	105	14%	637	86%	106	14%
AFOSI		588	576	98%	12	2%	575	98%	13	2%
Air Force SF		155	62	40%	93	60%	62	40%	93	60%
Marine Corps		129	92	71%	37	29%	83	64%	46	36%
Total		2,502	1,901	76%	601	24%	1,722	69%	780	31%

CID – Army Criminal Investigation Command
 MP – Military Police
 NCIS – Naval Criminal Investigative Service
 Navy SF – Navy Security Forces

AFOSI – Air Force Office of Special Investigations
 Air Force SF – Air Force Security Forces
 Marine Corps – Military Police and Criminal Investigations Division



Results in Brief

Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations

Findings (cont'd)

Within the Services, the Army, Navy, and Marine Corps had more missing fingerprint cards and final disposition reports. The Army had 262 (28 percent) missing fingerprint cards and 385 (41 percent) missing final disposition reports. The Navy had 197 (29 percent) missing fingerprint cards and 243 (36 percent) missing final disposition reports. The Marine Corps had 37 (29 percent) missing fingerprint cards and 46 (36 percent) missing final disposition reports.

Recommendations

We recommend that the Secretaries of the Army, Navy, and Air Force ensure that all fingerprint cards and final disposition reports that we identified as not submitted during the period of our review, from 2015 through 2016, be promptly submitted to the FBI CJIS.

We recommend that the Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer immediately perform a comprehensive review of their criminal investigative databases and files to ensure that all required fingerprint cards and final disposition reports for qualifying offenses at least to 1998 have been submitted to FBI CJIS in compliance with DoD and FBI requirements. We recommend that the review extend back to at least 1998 because that is when DoD policy required the Military Services to submit such qualifying fingerprints and final disposition reports. We recognize that all these records may not still be available, but we recommend the reviews determine what information can and should be submitted.

We recommend that the Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer take prompt action to institute command, supervisory, and management oversight controls to verify

compliance with fingerprint card and final disposition report submission requirements, in the past and in the future, and also ensure that such compliance is included as a special interest item in Service Inspector General inspections.

We recommend that the Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer conduct a comprehensive review of their criminal history reporting programs to ensure fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, the DoD policy covering the submission of fingerprints and final disposition reports, and are being implemented.

We recommend that the Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

Management Comments and Our Response

The Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer agreed with our recommendations. They also described actions they have begun taking and steps they intend to take to fully implement the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Secretary of the Army		A.1.a, A.1.b, A.1.c, A.1.d, A.1.e, B.1.a, B.1.b, B.1.c, B.1.d, B.1.e, B.1.f	
Secretary of the Navy		C.1.a, C.1.b, C.1.c, C.1.d, C.1.e, D.1.a, D.1.b, D.1.c, D.1.d, D.1.e, D.1.f, G.1.a, G.1.b, G.1.c, G.1.d, G.1.e	
Secretary of the Air Force		E.1.a, E.1.b, E.1.c, E.1.e, F.1.a, F.1.b, F.1.c, F.1.d, F.1.e, F.1.f	
Under Secretary of Defense for Intelligence		H.1.a, H.1.b, H.1.c, H.1.d	
Deputy Chief Management Officer		H.1.a, H.1.b, H.1.c, H.1.d	

Note: The following categories are used to describe agency management’s comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.





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

December 4, 2017

MEMORANDUM FOR SECRETARY OF THE ARMY
SECRETARY OF THE NAVY
SECRETARY OF THE AIR FORCE
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DEPUTY CHIEF MANAGEMENT OFFICER

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by
Military Service Law Enforcement Organizations (Report No. DODIG-2018-035)

We conducted this evaluation from February 2017 through October 2017, in accordance with the "Quality Standards for Inspection and Evaluation," published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

The Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer agreed with our recommendations. They also described actions they have begun taking and what steps they intend to take to fully implement the recommendations.

In addition, we considered management technical comments on a draft of this report when preparing the final report. We made minor factual corrections in response to some of those comments.

Comments from Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense for Intelligence; and the Deputy Chief Management Officer were responsive to the recommendations. We request that each regularly keeps us informed of its progress in implementing the recommendations.

We intend to follow up on the implementation of the recommendations and the steps each is taking to implement the recommendations.

If you have any questions or would like to meet to discuss the evaluation further, please contact SSA Jeff Bennett at (703) 699-5667. We appreciate the cooperation and assistance we received during the evaluation.

A handwritten signature in cursive script that reads "Glenn A. Fine".

Glenn A Fine
Principal Deputy Inspector General
Performing the Duties of the Inspector General

cc:
GENERAL COUNSEL, DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT
AND COMPTROLLER)

AUDITOR GENERAL, DEPARTMENT OF THE ARMY
INSPECTOR GENERAL, DEPARTMENT OF THE ARMY
JUDGE ADVOCATE GENERAL, U.S. ARMY
NAVAL INSPECTOR GENERAL
JUDGE ADVOCATE GENERAL, U.S. NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
INSPECTOR GENERAL, DEPARTMENT OF THE AIR FORCE
JUDGE ADVOCATE GENERAL, U.S. AIR FORCE
COMMANDER, UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
INSPECTOR GENERAL OF THE MARINE CORPS
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
DIRECTOR, PENTAGON FORCE PROTECTION AGENCY
COMMANDING GENERAL, UNITED STATES ARMY CRIMINAL
INVESTIGATION COMMAND
PROVOST MARSHAL GENERAL OF THE ARMY
COMMANDER, MARINE CORPS INSTALLATIONS COMMAND
STAFF JUDGE ADVOCATE TO THE COMMANDANT, U.S. MARINE CORPS
DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE
COMMANDER, AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
COMMANDER, AIR FORCE SECURITY FORCES CENTER
DIRECTOR, AIR FORCE SECURITY FORCES

Contents

Introduction

Objective.....	1
Background.....	1

Findings

Finding A. Army CID.....	7
Discussion.....	7
Recommendations, Management Comments, and Our Responses.....	10
Finding B. Army Military Police.....	12
Discussion.....	12
Recommendations, Management Comments, and Our Response.....	14
Finding C. NCIS.....	16
Discussion.....	16
Recommendations, Management Comments, and Our Response.....	18
Finding D. Navy Security Forces.....	20
Discussion.....	20
Recommendations, Management Comments, and Our Response.....	22
Finding E. AFOSI.....	25
Discussion.....	25
Recommendations, Management Comments, and Our Response.....	27
Finding F. Air Force Security Forces.....	29
Discussion.....	29
Recommendations, Management Comments, and Our Response.....	31
Finding G. Marine Corps MP and CID.....	33
Discussion.....	33
Recommendations, Management Comments, and Our Response.....	35

Additional Recommendations to Other

DoD Components	37
Recommendations, Management Comments, and Our Response.....	37

Overall Conclusions	40
----------------------------------	----

Contents (cont'd)

Appendixes

Appendix A. Scope and Methodology	43
Use of Computer-Processed Data	44
Appendix B. Qualifying Offenses	46
Appendix C. Prior Coverage	49
Appendix D. Management Comments	55
Secretary of the Army	55
Secretary of the Navy	59
NCIS	60
CNIC	62
USMC	64
Secretary of the Air Force	68
AFOSI	68
Air Force Security Forces	71
Under Secretary of Defense for Intelligence	74
Deputy Chief Management Officer	76
Defense Criminal Investigation Service	77
Acronyms and Abbreviations	78

Introduction

Objective

The objective of this evaluation was to determine whether the Military Services Law Enforcement Organizations (LEOs) had submitted:

- a Federal Document 249, “Arrest and Institution Fingerprint Card,” for Service members convicted of qualifying offenses (hereafter referred to as “convicted offenders”) listed in DoD Instruction (DoDI) 5505.11, “Fingerprint Card and Final Disposition Report Submission Requirements,” between January 1, 2015, and December 31, 2016, to the Criminal Justice Information Services Division (CJIS) for entry in the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) database and,
- an FBI-Department of Justice (DOJ) Form R-84, “Final Distribution Report,” if required, for Service members convicted by court-martial of qualifying offenses between January 1, 2015, and December 31, 2016, to CJIS for entry in the NGI database.¹

The Military Service LEOs are the Army Criminal Investigation Command, Naval Criminal Investigative Service, Air Force Office of Special Investigations, Army Military Police, Navy Security Forces, Air Force Security Forces, and Marine Corps Military Police and Criminal Investigative Division.

Appendix A discusses our scope and methodology in more detail. Appendix B lists the qualifying offenses in DoDI 5505.11. Appendix C summarizes several prior DoD OIG evaluations that examine the DoD’s submission of criminal history information to the FBI. Appendix D provides the Military Services and the DoD components’ written responses to our recommendations.

Background

The CJIS manages the criminal history record information for the Federal Government. The FBI’s NGI database is a national computerized system for storing, comparing, and exchanging fingerprint data and criminal history information for law enforcement purposes.

¹ DoDI 5505.11 lists qualifying offenses within the instruction for which fingerprints are required to be submitted to CJIS. A full listing of those offenses are contained in Appendix B to this report. Fingerprints are required to be submitted when probable cause exists to believe that the person has committed an offense, following coordination with the servicing SJA [Staff Judge Advocate] or legal advisor. In addition, a final disposition report must be submitted when final disposition is made against the subject. As explained in Appendix A, our review examined only those cases where the subject was convicted of a qualifying offense under DoDI 5505.11. We excluded from our sample those cases where there was no conviction, although such fingerprints may need to be submitted as well, and are covered by our recommendations to the Services.

This evaluation is the second recent evaluation of Military Service Law Enforcement Organizations (hereafter referred to as “LEOs”) compliance with fingerprint card and final disposition report data submission requirements.

In February 2015, the DoD OIG evaluated the Navy, Air Force, and Marine Corps to determine whether fingerprint cards and final disposition reports for a total of 1,102 Military Service members convicted of qualifying offenses between June 1, 2010, and October 31, 2012, were submitted to the FBI CJIS (Report No. DoDIG-2015-081).² DoD OIG found 304 of 1,102 (28 percent) fingerprint cards and 334 of 1,102 (30 percent) final disposition reports were missing. DoD OIG determined that the Navy failed to submit 68 of 317 (21 percent) required fingerprint cards and 80 of 317 (25 percent) required disposition reports. The Air Force failed to submit 110 of 358 (31 percent) required fingerprint cards and 113 of 358 (32 percent) required disposition reports and the Marine Corps failed to submit 126 of 427 (30 percent) required fingerprint cards and 141 of 427 (33 percent) required final disposition reports.

A prior DoD OIG evaluation conducted in 1997, found that between December 1995 and July 1996, the MCIOs did not consistently submit criminal history data to the FBI criminal history files. Based on the results of statistical sampling, DoD OIG determined that the Army failed to submit fingerprint cards to the FBI in approximately 82 percent of its cases; the Navy did not submit fingerprint cards in 83 percent of its cases; and the Air Force did not submit fingerprint cards in 38 percent of its cases. In addition, the Army did not submit final disposition reports in 79 percent of its cases; the Navy did not submit final disposition reports in 94 percent of its cases; and the Air Force did not submit final disposition reports in 50 percent of its cases.

In addition, in other DoD OIG evaluations, the DoD OIG determined that the Military Services were not consistently or uniformly submitting other required data from criminal investigations for inclusion in the FBI’s databases.

For example, as discussed in Appendix C, in Report No. DoDIG-2015-011, “Evaluation of the Defense Criminal Investigative Organizations’ Defense Incident-Based (DIBRS) Reporting and Reporting Accuracy,” October 29, 2014, the DoD OIG determined that the DoD was not reporting criminal incident data, such as the nature and types of specific offenses committed during the identified incident, characteristics of the victims, and information regarding the offenders and any other suspects arrested in connection with the incident to the FBI for inclusion in the annual Uniform Crime Reports, as required by Federal law.

² During the February 2015 evaluation, we did not examine U.S. Army fingerprint card and final disposition submission compliance because of United States Army Crime Record Center (USACRC) and FBI data validation limitations.

Also, in Report No. 2014-029, “Review of Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations,” February 27, 2014, the DoD OIG determined that the DoD did not submit 279 of 3,490 (8 percent) (excludes U.S. Coast Guard submission) required DNA samples to the United States Army Criminal Investigation Laboratory (USACIL) for inclusion in the Combined DNA Index System (CODIS) during our evaluation sample period of June 1, 2010, through October 31, 2012. The DoD had an overall noncompliance rate of 8 percent.³

In another example, Report No. DoDIG-2013-091, “Evaluation of Military Criminal Investigative Organizations’ Sexual Assault Investigations,” July 9, 2013, the DoD OIG evaluated a sample of 501 Army, Navy, Air Force, and Marine Corps subjects investigated for sexual assault, between February 2012 and September 2012 that were required to have their fingerprints collected and submitted to the FBI CJIS. DoD OIG determined that 101 of 501 (20 percent) fingerprints were not collected by MCIOs, or were collected, but were not submitted to the FBI. The MCIO’s had an overall fingerprint collection noncompliance rate of 20 percent.

See Appendix C for the results of these evaluations.

The Historical Development of DODI 5505.11

DoD Memorandum, March 25, 1987

On March 25, 1987, DoD OIG issued Criminal Investigations Policy Memorandum Number (CPM No. 10), “Criminal History Data Reporting Requirements.” The purpose of this memorandum was to establish policies and procedures for the Defense Criminal Investigative Organizations (DCIO) to report offender criminal history data to the FBI.⁴ The memorandum required the DCIOs to submit to the FBI offender criminal history data for all Military Service members they investigated for any qualifying offenses, and who were subjects of any resultant judicial or non-judicial military proceeding. The requirement to submit criminal history data applied only to the DCIOs and did not apply to other DoD law enforcement agencies.

³ USACIL is the only full-service forensic laboratory in DoD that provides forensic support to DoD criminal investigative organizations and the USCGIS. It is the DoD executive agent for DNA analysis of samples collected from military arrestees and convicted offenders. The term CODIS is used generically to describe the FBI program for supporting criminal justice DNA databases and the software used to operate the databases. CODIS contains DNA profiles on arrestees, convicted offenders, unsolved crime scene evidence, and missing persons.

⁴ The DCIOs are the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the Defense Criminal Investigative Service. The Defense Criminal Investigative Service is the criminal investigative arm of the Inspector General, DoD.

DoD Memorandum, November 14, 1996

On November 14, 1996, the DoD OIG issued a memorandum titled, “*Evaluation of Compliance with DoD Criminal Investigations Policy Memorandum No. 10, Criminal History Data Reporting Requirements.*” This memorandum noted the requirement under the National Defense Authorization Act of 1996 for the Secretary of Defense to report to Congress the consistency with which fingerprint cards and final disposition forms were reported by the DCIOs to the FBI. The memorandum also reported the initial results of the DoD OIG’s ongoing evaluation, which identified a high level of noncompliance with the reporting requirements by the MCIOs. The memorandum advised that the DoD OIG would issue a new DoD Instruction applicable to DoD LEOs addressing that criminal history data should be reported. Until the Instruction was issued, the memorandum directed all DoD agencies to report offender criminal history data to the FBI.

DoDI 5505.11, December 1, 1998

On December 1, 1998, the DoD IG published DoDI 5505.11, “*Fingerprint Card and Final Disposition Report Submission Requirements,*” which implemented policy, assigned responsibilities, and prescribed procedures for LEOs to report offender criminal history data to the FBI CJIS.⁵ It required the DCIOs and all other DoD criminal investigative and police organizations to submit to the FBI offender criminal history data for all Military Service members investigated for qualifying offenses listed within the instruction. The instruction also required LEOs to collect fingerprints and all additional case information from military suspects under investigation for qualifying offenses and annotate them on Federal Document 249 (FD-249), “Arrest and Institution Fingerprint Card,” (hereafter referred to as “fingerprint card”), within 15 days of when a command initiated military judicial proceedings, or command action was taken in non-judicial proceedings. In addition, the instruction required the reporting of final disposition information on an FBI-Department of Justice Form R-84, Final Disposition Report, (hereafter referred to as “final disposition report”), or an electronic data transfer equivalent, within 15 days after final disposition of judicial or non-judicial proceedings.

⁵ Beginning in 1999, the CJIS Division operated and maintained the Integrated Automated Fingerprint Identification System (IAFIS) as the FBI criminal and civil fingerprint history database. In 2014, the FBI replaced IAFIS with the NGI. <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

DoDI 5505.11 Revisions

The DoDI 5505.11 was revised several times over the last two decades.

For example, on June 20, 2006, the DoD published a revision which broadened the application of DoDI 5505.11 to civilians investigated for any offense other than non-serious offenses as defined by the FBI. On July 9, 2010, the published version extended the required submission of fingerprints and criminal history data to foreign national subjects of investigations. It also updated required offender criminal history data submission when an agent or other law enforcement investigator (in consult with a legal advisor, if necessary) determined that probable cause existed to believe that the subject had committed an offense. Finally, the April 15, 2012, DoDI 5505.11 revision required the submission of all fingerprints to the FBI electronically. If no electronic submission capability existed at the LEO, the revision required the development of procedures to convert fingerprints from a hard copy FD-249 to an electronic format.

NGI Database

Section 534, title 28, United States Code, states that:

[t]he Attorney General [FBI] shall acquire, collect, classify, and preserve identification, criminal identification, crime, and other records... [and] exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States . . . cities, and penal and other institutions.⁶

The NGI database's primary function is to provide the FBI with an automated fingerprint identification and criminal history reporting system. The FBI NGI database is a national computerized system for storing, comparing, and exchanging fingerprint data and criminal history information.⁷

Federal, state, and local law enforcement agencies submit fingerprint cards and criminal history information to the NGI database. The NGI database provides automated fingerprint search capabilities, electronic image storage, and electronic exchange of fingerprints. Information in the NGI database is shared with criminal justice agencies nationwide through the FBI CJIS National Crime Information Center (NCIC).⁸ Specifically, among other uses, NGI information is checked by Federal Firearms Licensees to instantly determine, through the FBI CJIS National Instant Criminal Background Check System (NICS), whether a prospective buyer is eligible to buy firearms.⁹

⁶ 28 United States Code §534. Acquisition, preservation, and exchange of identification records and information.

⁷ FBI CJIS "Fingerprints and Other Biometrics" webpage at <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi>.

⁸ FBI CJIS "National Criminal Information Center (NCIC)" webpage at <https://www.fbi.gov/services/cjis/ncic>.

⁹ FBI CJIS "National Instant Criminal Background Check System (NICS)" webpage at <https://www.fbi.gov/services/cjis/nics>.

Any missing fingerprint card and final disposition report can have serious, even tragic, consequences, as may have occurred in the recent church shooting in Texas. The failure to populate FBI databases with all the required fingerprint records can result in someone purchasing a weapon who should not. It can also hinder criminal investigations and potentially impact law enforcement and national security interests.

Each criminal arrest for which the FBI CJIS has received a fingerprint submission should also have a disposition in the NGI database. According to the FBI's website,

[t]he FBI defines a disposition as the formal or informal conclusion of an arrest or charge at whatever stage it occurs in the criminal justice system. A disposition reports the court's findings and can include information as to whether an arrest charge has been modified or dropped.¹⁰

The LEOs use the fingerprint cards and the final disposition reports to document and submit fingerprint cards and case information to the FBI CJIS for entry into the NGI database.

The following section discusses the results of our evaluation. We provide detailed results, broken down by each Service.

¹⁰ <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/arrest-disposition-submission>.

Finding A

Army CID

Army CID did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 159 of 768 (21 percent) required fingerprint cards and 264 of 768 (34 percent) required final disposition reports.

Discussion

Special agents assigned to the U.S. Army Criminal Investigation Command (CID) typically investigate felony crimes in the Army.

The CID fingerprint card and final disposition report submission and noncompliance rates are shown in Table 1.

Table 1. The CID Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	768
Fingerprint Cards in NGI	609
Fingerprint Cards Not in NGI	159
Fingerprint Card Noncompliance Rate	21%
Final Disposition Reports in NGI	504
Final Disposition Reports Not in NGI	264
Final Disposition Noncompliance Rate	34%

Source: Service JAGs, FBI CJIS, and CID.

Fingerprint Card Collection Process

Until mid-December 2015, the CID collected fingerprint cards using hardcopy fingerprint cards. The CID field units submitted fingerprint cards to the U.S. Army Crime Record Center (USACRC), which scanned the fingerprint cards, manually entered arrest-related information, and submitted the fingerprint cards and the arrest related-information electronically to the FBI CJIS.¹¹ The USACRC representative told us that fingerprint cards from field units were scanned and transmitted to the FBI CJIS upon receipt. However, we determined that the USACRC

¹¹ The USACRC is the Army proponent responsible for all Army fingerprint card and final disposition submissions (CID and Army MPs). The USACRC is responsible for forwarding fingerprint cards to the FBI CJIS.

did not have a mechanism to ensure that the field units were submitting all of the fingerprint cards as required by DoDI 5505.11. In addition, the USACRC did not have a procedure to track fingerprint cards that it had rejected and returned to the field units for recollection or a mechanism to track whether the recollected fingerprint cards were resubmitted to USACRC.¹²

In mid-December 2015, the CID distributed its first electronic fingerprint scanning equipment and software (hereafter referred to as “live scan”) to some field units. Within 6 months, it equipped the remainder of its field units with live scan equipment. These electronic, live scan units provided field units with the capability to submit fingerprint cards electronically to the FBI CJIS.

If final disposition data were not known at the time the fingerprint card was submitted to the FBI CJIS the field unit should have submitted a final disposition report once the final disposition was determined. CID policy directs its field units to submit final disposition reports directly to the FBI CJIS. However, the Army had no mechanism to ensure that the field units were submitting all of the final disposition reports as required by DoDI 5505.11.

Fingerprint Card Submission Guidance and Training

We reviewed CID Regulation 195-1, “Criminal Investigation Operational Procedures,” January 2, 2015, and determined it provided guidance consistent with DoDI 5505.11 for field investigators to comply with fingerprint card and final disposition report submission requirements.

On March 9, 2015, and July 13, 2016, the CID issued command-wide memorandums to provide the field units with additional guidance on the preparation and disposition of fingerprint cards and using live scan technology. We reviewed CID regulations and determined that the regulations provided guidance consistent with DoDI 5505.11 for field investigators to comply with fingerprint card and final disposition report submission requirements.

We also reviewed the U.S. Army Military Police School (USAMPS) training curriculum. USAMPS provides instruction for the Military Police Basic and Advanced Training Courses, the CID Special Agent Course (CIDSAC), and the Military Police Investigator (MPI) course. CIDSAC graduates become special agents with the Army CID or Marine Corps CID. MPI course attendees include Army Military Police (MP), Navy Security Forces, Air Force Security Forces, and

¹² The USACRC staff provided us the following reasons fingerprint cards have been rejected: fingerprint card not signed by the subject; missing information, i.e., date of offense, subject date of birth, or date of arrest; and illegible entries.

Marine Corps MPs. We found that the USAMPS fingerprint collection training focused on collecting fingerprints solely for evidentiary purposes, but does not teach students the requirement to submit fingerprint cards or final disposition reports to the FBI CJIS.

LEO Oversight

CID Regulation 1-201, "Organizational Inspection Program," March 12, 2013, states that a CID Inspector General (IG) focuses on compliance with standards contained in CID Regulation 195-1. CID Regulation 195-1, Appendix D, establishes standards for the CID investigation program. One standard is that supervisors are to ensure that CID field elements are preparing and forwarding fingerprint cards to USACRC and final disposition reports to the FBI CJIS.

We reviewed a CID command IG inspection report, which indicated that fingerprint card and final disposition data submission compliance is reviewed during IG inspections.

In August 2017, we asked the USACRC Director why fingerprint card and final disposition submission rates were deficient if the CID IG is inspecting field units to assess submission compliance. The USACRC Director provided the following reasons for the fingerprint card and final disposition report submission rates:

We are in non-compliance due to the fact the CID field elements are not following guidance provided by DOD Instructions, [U.S. Army] Criminal Investigations Division regulations and policy concerning submission of fingerprints and dispositions. Fingerprints may be collected but not forwarded to the FBI. Additionally, with the implementation of Live Scan [sic] the fingerprints are being sent directly to FBI CJIS. The Crime Records Center no longer has visibility on what [which] prints have gone [been submitted] or their disposition.

The Director told us that USACRC is developing a reporting mechanism within the Army Law Enforcement Reporting and Tracking System (ALERTS) database to track fingerprint card submissions and final disposition reports.¹³ However, the Director did not know when the database update would be completed.

¹³ ALERTS is the primary case management system for all Army law enforcement professionals. This system provides the Army with an integrated case management system for law enforcement, supporting both the MP and the CID.

Recommendations, Management Comments, and Our Responses

Recommendation A.1

We recommend that the Secretary of the Army take prompt action to:

- a. **Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 159 CID fingerprint cards and 264 CID final disposition reports that are not in the FBI Next Generation Identification database.**
- b. **Immediately perform a comprehensive review of all Army criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**
- c. **Ensure that CID command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in CID IG inspections, and is actually conducted.**
- d. **Conduct a comprehensive review of CID criminal history reporting programs to ensure fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and are being implemented.**
- e. **Also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**

Army Comments

The Army, including the Office of the Provost Marshal General (OPMG), Criminal Investigation Command (CID), and Installation Management Command reviewed our findings and recommendations and consolidated its response. The Army agreed with the recommendations. In addition, the Army described steps it is taking to implement the recommendations. These steps include coordinating with officials at both the National Crime Information Center (NCIC) and the National Instant Criminal Background Check System (NICS) to submit automated data regarding felony convictions, including drug offenders and convicted domestic violence offenders; actively reviewing data; submitting final disposition reports; and assisting affected Army commands to identify and address resourcing needs for submission of automated fingerprint cards via LiveScan technology. The Army's

projected timeline for completion of this effort is no later than the 3rd Quarter of Fiscal Year 2018. Additionally, the Army stated that it is reviewing its law enforcement database to ensure missing fingerprint cards and final disposition reports are reported to the FBI in compliance with statutory, DoD, and FBI requirements. According to the Army, this review will also identify and address gaps and shortcomings in policy, resources, and manning, as well as address shortfalls identified in the submission of DNA to Federal databases. In addition, the Army is developing a tracking system that compares offenders against LiveScan submissions to ensure that fingerprint cards and final disposition reports are submitted Army wide. Finally, the Army stated that it will ensure that the CID OIG continues to assess compliance with DoDI 5505.11 requirements.

Our Response

Comments from the Army addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Army describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that CID has completed agreed upon corrective actions.

Finding B

Army Military Police

Army Military Police did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 103 of 180 (57 percent) required fingerprint cards and 121 of 180 (67 percent) required final disposition reports.

Discussion

Military Police (MP) and MP Investigators typically investigate misdemeanor crimes in the Army such as petty theft, simple assault, and traffic crimes.

Army MP fingerprint card and final disposition report submission and compliance rates are shown in Table 2.

Table 2. Army MP Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	180
Fingerprint Cards in NGI	77
Fingerprint Cards Not in NGI	103
Fingerprint Card Noncompliance Rate	57%
Final Disposition Reports in NGI	59
Final Disposition Reports Not in NGI	121
Final Disposition Noncompliance Rate	67%

Source: Service JAGs, FBI CJIS, and CID.

Note: The U.S. Army Crime Records Center, a unit subordinate to the CID, is the proponent for Army law enforcement reporting, including fingerprint procedures, and provided information to identify convicted offenders investigated by Army MPs.

Fingerprint Card Collection Process

During the evaluation period, Army MPs used hardcopy fingerprint cards to collect fingerprints for submission to the USACRC. The USACRC staff scanned fingerprint cards, manually entered arrest-related information into live scan, and then submitted the fingerprint cards and the arrest-related information electronically to the FBI CJIS.¹⁴

The USACRC representative told us that fingerprint cards from MP field units were scanned and transmitted to the FBI CJIS by USACRC upon receipt. However, we determined that the USACRC did not have a mechanism to ensure that the field units were submitting all of the fingerprint cards as required by DoDI 5505.11. In addition, the USACRC did not have a procedure to track fingerprint cards that it had rejected and returned to MP field units for recollection or a mechanism to track whether the recollected fingerprint cards were resubmitted to the USACRC. MP field units mailed final disposition reports to the USACRC for submission to FBI CJIS. However, the Army had no mechanism to ensure that the field units were submitting all of the final disposition reports as required by DoDI 5505.11.

Fingerprint Card Submission Guidance and Training

We reviewed Army Regulation (AR) 190-45, “Law Enforcement Reporting,” March 30, 2007, and September 27, 2016, and determined that it provided guidance that conflicts with DoDI 5505.11. DoDI 5505.11 requires fingerprint card submission upon a probable cause determination for military members investigated for qualifying offenses. AR 190-45 states that fingerprints, “will be sent to the Director, USACRC, and processed with the MPR [Military Police Report]” upon case closure. It does not state that fingerprint cards should be submitted when a probable cause determination has been made.¹⁵ This process, in which case files and fingerprint cards are submitted to the USACRC only at the end of the investigation, conflicts with DoDI policy and delays fingerprint card submissions.¹⁶

We also reviewed the USAMPS training curriculum. We found that the USAMPS fingerprint collection training focused on collecting fingerprints solely for evidentiary purposes, but does not teach students the requirement to submit fingerprint cards or final disposition reports to FBI CJIS.

¹⁴ During our evaluation, the Fort Rucker, Alabama MP stations developed electronic submission capability.

¹⁵ DoDI 5505.11 defines probable cause determination as a “[d]etermination that there are reasonable grounds to believe that an offense has been committed and that the person to be identified as the offender committed it.”

¹⁶ The Office of the Provost Marshal General of the Army is responsible for issuing AR 190-45.

LEO Oversight

As part of our evaluation, we interviewed an IMCOM Law Enforcement Specialist with the IMCOM Command Provost Marshal Protection Directorate. The Law Enforcement Specialist advised us that IMCOM headquarters routinely inspected MP stations as part of its physical security and law enforcement organizational inspection program. We therefore examined the IMCOM physical security and law enforcement inspection checklist, which included a line item for inspectors to validate whether criminal history data are being submitted to the USACRC for transmittal to the FBI CJIS.

We asked the IMCOM Specialist why IMCOM's fingerprint card and final disposition report submission rates were deficient if IMCOM headquarters routinely conducts inspections. He told us when IMCOM headquarters staff members conduct inspections, they do not conduct a 100 percent review of all case files. Rather, they review a sample of case files that are ready to be sent to the USACRC. The inspection team checks case files to ensure that the cases are complete, including checking for fingerprint cards and R-84s. However, we found that the headquarters routine inspections, although designed to identify compliance, did not identify the fingerprint submission deficiencies.

The IMCOM representative told us he thought that not having live scan technology contributed to IMCOM's deficient compliance rates. We agree live scan would likely improve submission rates because unacceptable fingerprint cards are immediately rejected. The immediate rejection allows a subject's fingerprints to be re-collected while subjects are still present and the fingerprints can then be immediately re-entered into the system. However, the absence of live scan technology does not excuse Army MP units' failure to collect and submit hard-copy fingerprint cards and final disposition reports to USACRC for eventual entry into FBI CJIS.

Recommendations, Management Comments, and Our Response

Recommendation B.1

We recommend that the Secretary of the Army take prompt action to:

- a. **Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 103 IMCOM fingerprint cards and 121 installation final disposition reports that are not in the Federal Bureau of Investigation Next Generation Identification database.**

- b. Immediately perform a comprehensive review of all IMCOM criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses since at least to 1998 have been reported to FBI CJIS in compliance with DoD and FBI requirements.**
- c. Ensure that IMCOM command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in Army IG inspections, and is actually conducted.**
- d. Conduct a comprehensive review of IMCOM criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.**
- e. Also ensure that other required investigative and criminal history information, such as, criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**
- f. Direct the U.S. Army Provost Marshal General to revise AR 190-45 to align with the fingerprint card and final disposition report submission requirements in DoDI 5505.11.**

Army Comments

In the Army's consolidated response, the Office of the Provost Marshal General noted that, in addition to the efforts described above, the Army published an update to AR 190-45 on September 27, 2016, which requires that fingerprint cards are submitted when probable cause has been determined. The Army stated its intention to further update AR 190-45 to clearly define the process and procedures for submitting fingerprint cards.

Our Response

Comments from the Army addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Army describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that Army MPs have completed agreed upon corrective actions.

Finding C

NCIS

NCIS did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 159 of 631 (25 percent) required fingerprint cards and 203 of 631 (32 percent) required final disposition reports.

Discussion

Special agents assigned to the Naval Criminal Investigative Service (NCIS) typically investigate felony investigations within the Navy and Marine Corps.

NCIS fingerprint card and final disposition report submission and compliance rates are shown in Table 3.

Table 3. NCIS Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	631
Fingerprint Cards in NGI	472
Fingerprint Cards Not in NGI	159
Fingerprint Card Noncompliance Rate	25%
Final Disposition Reports in NGI	428
Final Disposition Reports Not in NGI	203
Final Disposition Noncompliance Rate	32%

Source: Service JAGs, FBI CJIS, and NCIS.

Fingerprint Card Collection Process

The NCIS field offices that regularly processed criminal investigations are equipped with live scan and submitted fingerprint cards directly to the FBI CJIS. The field offices not equipped with live scan collected fingerprints use hardcopy fingerprint cards, which are submitted to NCIS headquarters for scanning and submission to the FBI CJIS database. All NCIS offices were directed to submit final disposition reports directly to the FBI CJIS database. However, we determined that there was no mechanism to ensure that the field units were submitting all of the fingerprint cards and final disposition reports required by DoDI 5505.11.

The NCIS Live Scan Coordinator told us that NCIS anticipates using a “booking” system being designed by Army CID to collect biographical data, fingerprints, and photographs. He said that NCIS anticipates this booking system will simplify the submission process and improve compliance rates. He said that this booking system will include the capability to submit final disposition reports electronically, identify charges requiring fingerprint card submission, and display posters and manuals that will explain the system and policies to investigators and supervisors.

Fingerprint Card Submission Guidance and Training

We reviewed NCIS instructions and determined that they provide guidance consistent with DoDI 5505.11 for field investigators to comply with fingerprint card and final disposition report submission requirements. NCIS-3, “Criminal Investigations,” Chapter 37, “Biometrics,” January 2014, describes fingerprint card collection and submission and final disposition report submission requirements.

On June 3, 2016, the NCIS Biometrics Division published additional guidance titled, “Naval Criminal Investigative Service Identity Live Scan Work Instruction.” This guidance provides step-by-step procedures on how the NCIS Federal law enforcement agency processes fingerprint cards and final disposition reports.

According to the NCIS Live Scan Coordinator, the NCIS Biometrics Division trains and tests Special Agent Basic Training students on the use of live scan for collecting and submitting fingerprint cards and final disposition reports.

LEO Oversight

The NCIS Live Scan Coordinator told us that NCIS personnel oversee fingerprint card and final disposition report submission at first-line supervisor and supervisory special agent levels. He said supervisors use two checklists to review cases and monitor submission compliance: NCIS Form 5580/101, “NCIS Standardized Case Review Sheet,” and NCIS Form 5580/54, “NCIS Case Tracking and File Management Form.”

The NCIS Live Scan Coordinator also said the NCIS Office of Inspector General (OIG) reviews the “NCIS Standardized Case Review Sheets” during its inspections to verify that fingerprints were collected, but it does not verify that the fingerprint cards or final disposition reports were submitted. The NCIS Live Scan Coordinator said the NCIS OIG also did not document fingerprint cards or final disposition reports submission in its official inspection reports.

In addition, the NCIS Deputy IG told us that missing fingerprint cards were noted as a finding at two field offices during our evaluation period. In each case, the NCIS OIG team instructed the field office to take appropriate action to ensure fingerprint collection was properly documented. In a follow-up message on October 31, 2017, the NCIS OIG told us the field offices had corrected all of the deficiencies except one. Fingerprints will be collected and submitted in early November 2017, when the sailor returns from deployment afloat.

We asked the NCIS Live Scan Coordinator why NCIS fingerprint card and final disposition submission rates were deficient, given the prescribed directives for supervisors to follow internal oversight policy and the NCIS OIG policy to check fingerprint cards during its inspections. He attributed the deficient fingerprint card and final disposition submission rates to: (1) fingerprints being collected but not submitted to, or rejected by, the FBI CJIS and (2) NCIS field agents not being aware of final disposition report submission requirements. He also said that planned initiatives, such as the new booking system, should help with compliance by enabling the electronic submission of final disposition reports. Additionally, he told us that as a result of our evaluation, NCIS had identified 26 active duty convicted offenders still under Navy control whose fingerprint cards had not been collected and submitted to the FBI CJIS. He said that the NCIS is in the process of collecting those fingerprint cards.

Recommendations, Management Comments, and Our Response

Recommendation C.1

We recommend that the Secretary of the Navy take prompt action to:

- a. Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 159 NCIS fingerprint cards and 203 NCIS final disposition reports that are not in the Federal Bureau of Investigation Next Generation Identification database.**
- b. Immediately perform a comprehensive review of all NCIS criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**
- c. Ensure that NCIS command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in NCIS IG inspections, and is actually conducted.**

- d. Conduct a comprehensive review of NCIS criminal history reporting programs to ensure all applicable agency policy, training, fingerprinting, and final disposition report submission processes are consistent with DoDI 5505.11, and have been implemented.**
- e. Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**

Navy Comments

The Navy, including NCIS and the Commander of Navy Installations Command reviewed our findings and recommendations. The Navy agreed with the recommendations.

NCIS described steps it is taking to implement the recommendations, including developing a “Fingerprint Verification Plan” to correct previous fingerprint submission deficiencies and to prevent future submission failures. The plan includes a field office review of open cases and closed case files within the last 12 months to verify submission of fingerprint cards, and a NCIS validation of the results of the review.

In addition, the Navy stated that NCIS Headquarters will query all historical case files from January 1, 1998 to September 30, 2016 to determine which have fingerprints submitted to the NCIC, and will provide missing final disposition reports, if any. The estimated completion date for these efforts is December 8, 2017. NCIS will also review historical cases to identify cases in which the command took punitive action against the offender but failed to submit fingerprint cards. For cases in which fingerprint cards cannot be located, NCIS will submit final disposition reports directly to the NICS for entry into the database. Finally, NCIS will submit missing final disposition reports for historical cases where fingerprint cards were submitted to the NCIC but the final disposition reports are missing. The Navy stated that these efforts are ongoing.

Our Response

Comments from the Navy addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Navy describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that NCIS has completed agreed upon corrective actions.

Finding D

Navy Security Forces

Navy Security Forces did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 38 of 51 (75 percent) required fingerprint cards and 40 of 51 (78 percent) required final disposition reports.

Discussion

The Navy Security Forces personnel assigned to Commander, Naval Installations Command (CNIC) typically investigate misdemeanor crimes in the Navy, such as petty theft, simple assault, and traffic crimes.

Navy Security Forces fingerprint card and final disposition report submission and compliance rates are shown in Table 4.

Table 4. Navy Security Forces Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	51
Fingerprint Cards in NGI	13
Fingerprint Cards Not in NGI	38
Fingerprint Card Noncompliance Rate	75%
Final Disposition Reports in NGI	11
Final Dispositions Not in NGI	40
Final Disposition Noncompliance Rate	78%

Source: Service JAGs, FBI CJIS, and NCIS.

Note: The NCIS Biometrics Division staff had access to the Navy Consolidated Law Enforcement Operations Center database and provided necessary CNIC report information.

Fingerprint Card Collection Process

Navy Security Forces personnel, assigned to the Commander, Navy Installations Command (CNIC) installations, were supposed to collect fingerprints on hardcopy fingerprint cards, which they mailed to NCIS headquarters for electronic scanning and submission to the FBI CJIS. The NCIS Biometrics Division Chief told us that if the forms were rejected, NCIS returned the fingerprint cards to the Navy Security

Forces office for recollection and resubmission.¹⁷ The NCIS staff keeps a log of rejected fingerprint cards and checks the status with the field units on a monthly basis. Navy Security Forces field units submitted final disposition reports directly to the FBI CJIS, rather than through NCIS.

Fingerprint Card Submission Guidance and Training

We reviewed Navy Security Forces guidance and determined that it provided guidance in conflict with DoDI 5505.11. As noted above, DoDI 5505.11 requires fingerprint card submission upon a probable cause determination for military members investigated for qualifying offenses. However, Navy Tactics, Techniques, and Procedures (NTTP), “Law Enforcement and Physical Security NTTP 3-07.2.3,” August 2011, incorrectly requires that fingerprint cards be submitted only after a command initiates military judicial proceedings or when command action is taken in a non-judicial punishment proceeding. Furthermore, it does not mention the DoDI 5505.11 requirement for coordination with an SJA or other legal advisor for a probable cause determination.

We also determined that Navy Security Forces did not have formal fingerprint card and disposition data collection and submission training for its investigators. When we asked a CNIC law enforcement representative why CNIC had no formal training, the CNIC Assistant Training Program Manager responded:

We consider this type of training On the Job Training (OJT) for those officers who are required to perform this function.

The US Navy uses a system referred to as Personnel Qualification Standards (PQS). The PQS Program is used by officer and enlisted personnel to obtain the minimum level of competency required to perform specific duties. . . .There are line items in the Law Enforcement PQS which outline Biometric fingerprint scanning, demonstration of how to use and the appropriate signature verifying completion of the task [sic].

We examined the Personnel Qualification Standards CNIC provided and found that it did not address fingerprint card or final disposition report submission requirements.

¹⁷ The NCIS Biometrics Division performs a full range of activities including device acquisition and management, operations development and support, biometrics training, and biometric-enabled intelligence analysis <http://www.ncis.navy.mil/MissionSupport/Pages/Biometrics.aspx>. The Biometrics Division Chief is a headquarters-based supervisory special agent.

Some Navy Security Forces personnel attend the MPI course at Army Military Police School and receive some fingerprint collection training. However, Army Military Police Investigations training focused on collecting fingerprints for comparison purposes, rather than the requirement to submit fingerprint cards and final disposition reports to the FBI CJIS.

LEO Oversight

The NTTP 3-07.2.3 requires both the NCIS Regional Investigations Coordinator and the Security Forces installation Security Officer to establish a case review process. The NTTP further states that the Regional Investigations Coordinator must have an effective program in place to ensure quality assurance review and maintenance of investigative files. The NTTP also requires supervisors to conduct biweekly case reviews and the Regional Investigations Coordinator to conduct periodic oversight case reviews with command investigators.¹⁸ The NTTP does not mention oversight of the fingerprint card and final disposition report submission process. Navy Security Forces guidance does not mandate oversight of fingerprint cards and final disposition report submissions at other leadership levels. The CNIC did not conduct any inspection relating to verifying compliance with fingerprinting policy or prepare any after-action reports regarding fingerprint submissions during our evaluation period.

The CNIC law enforcement representative told us that compliance was deficient because the Navy Security Forces did not have formal fingerprint or fingerprint card processing training for its investigators.

Recommendations, Management Comments, and Our Response

Recommendation D.1

We recommend that the Secretary of the Navy take prompt action to:

- a. Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 38 Navy Security Forces fingerprint cards and 40 Navy Security Forces final disposition reports that are not in the Federal Bureau of Investigation Next Generation Identification database.**

¹⁸ According to OPNAV [Chief of Naval Operations] Instruction 5530.14E, Change 2, "Navy Physical Security and Law Enforcement Program," September 23, 2014, a RIC (regional investigations coordinator) is an experienced NCIS special agent whose oversight responsibilities, "include, but is not limited to, training, investigative procedures, case management, investigator screening/selection, and investigative standardization. . . .RIC oversight and responsibilities will encompass all Navy investigators within the region." NTTP 3-07.2.3 also reflects, "Where regionalization has been implemented, the investigative responsibility will fall upon the regional investigations coordinator (RIC), with coordination between the RIC and the RSO [Regional Security Officer] and SO [Security Officer]."

- b. Immediately perform a comprehensive review of all Navy Security Forces criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**
- c. Ensure that Navy Security Forces command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in future IG inspections and is actually conducted.**
- d. Conduct a comprehensive review of Navy Security Forces criminal history reporting programs to ensure all applicable agency policy, training, fingerprinting, and final disposition report submission processes are consistent with DoDI 5505.11, and have been implemented.**
- e. Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**
- f. Direct the Commander of Naval Installations Command to revise NTTP 3-07.2.3 to align with fingerprint card submission requirements set forth in DoDI 5505.11.**

Navy Comments

The Navy agreed with our recommendations. Specifically, CNIC stated that, on November 9, 2017, CNIC initiated a comprehensive review of its criminal history reporting program, including policy, training, fingerprint equipment, fingerprints, and final disposition report submission processes, to ensure compliance with DoDI 5505.11. CNIC estimates completion of this review on December 30, 2017, and all corrective actions by June 30, 2018. The CNIC response stated that on November 20, 2017, CNIC directed all Navy Security Forces under its cognizance to conduct a review of all entries in the Navy Criminal Law Enforcement Operations Center (CLEOC) database for qualifying offenses and verify compliance of fingerprint card and final disposition report submission in the FBI CJIS database. CNIC estimates that missing fingerprint cards and final disposition reports will be submitted by January 31, 2018. CNIC also stated that they will ensure that command, supervisory, and management oversight controls verify compliance with DoDI 5505.11, and incorporate compliance verification as a special interest item in future IG inspections and conduct checks as part of the inspection cycle.

Our Response

Comments from the Navy addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Navy describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that Navy Security Forces has completed agreed upon corrective actions.

Finding E

AFOSI

AFOSI submitted most but not all the required fingerprint cards and final disposition reports. We determined that it failed to submit 12 of 588 (2 percent) required fingerprint cards and 13 of 588 (2 percent) required final disposition reports.

Discussion

Special agents assigned to Air Force Office of Special Investigations (AFOSI) typically investigate felony crimes in the Air Force.

AFOSI fingerprint card and final disposition report submission and compliance rates are shown in Table 5.

Table 5. AFOSI Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	588
Fingerprint Cards in NGI	576
Fingerprint Cards Not in NGI	12
Fingerprint Card Noncompliance Rate	2%
Final Disposition Reports in NGI	575
Final Disposition Reports Not in NGI	13
Final Disposition Noncompliance Rate	2%

Source: Service JAGs, FBI CJIS, and AFOSI.

Fingerprint Card Collection Process

AFOSI agents collected fingerprints using digital scanners. The software sends the electronic fingerprints directly to the FBI CJIS. Most AFOSI field offices that regularly process criminal investigations were equipped with digital scanners. For those AFOSI field offices not equipped with digital scanners, or when a field office's digital scanner was not operational, fingerprints were collected using hardcopy fingerprint cards and were mailed to headquarters AFOSI for submission to the FBI CJIS.

In addition, AFOSI's investigative database programming prevents closure of an investigation until an AFOSI supervisor certifies in the Investigative Information Management System (I2MS) database that the fingerprint cards and final disposition reports have been submitted to the FBI CJIS. All AFOSI field offices submit final disposition reports directly to the FBI CJIS.¹⁹

Fingerprint Card Submission Guidance and Training

We reviewed AFOSI Manual 71-121, "Processing and Reporting Investigative Matters," April 13, 2015, Incorporating Change 1, June 6, 2016 and determined it provided guidance consistent with DoDI 5505.11 for field investigators to comply with fingerprint card and final disposition report submission requirements.

We reviewed training documents from the U.S. Air Force Special Investigations Academy (USAFSIA) and determined that they also provided guidance consistent with DoDI 5505.11 for field investigators to comply with fingerprint card and final disposition report submission requirements. We determined that fingerprint card collection and submission procedures are taught during several classes at the AFOSI Basic Special Investigators Course (BSIC) and Advanced General Crimes Investigation Course (AGCIC). In particular, fingerprint card submission is highlighted during a 4-hour block of instruction for I2MS.

Fingerprint card submission is also taught during the 1-hour Subject Processing Procedures lecture and the "Web I2MS Case Closure" lesson. Students have opportunities to practice fingerprinting during the "Continuing Case Operations" and "Detachment Operations" classes. While attending the BSIC, students are provided with an I2MS Navigation and Documenting Guide that contains all the information needed to successfully submit fingerprint cards and final disposition reports. In addition, students receive refresher training on fingerprint card submission and final disposition reporting during the AGCIC.

LEO Oversight

In June 2017, AFOSI told us that it has several levels of oversight regarding fingerprint cards and final disposition reports submission to the FBI CJIS. Field agents and supervisors use two checklists to review cases and monitor submission compliance: the AFOSI Investigative Sufficiency Checklist and the AFOSI Closed Case Review Checklist. The Headquarters AFOSI, Performance Management Branch, also reviews the AFOSI Closed Case Review Checklist as an oversight function to identify and prevent deficiencies that are systemic across the command. Headquarters AFOSI developed a SMART-OSI [Strategic Management

¹⁹ I2MS is an activity-based automated information system used by AFOSI that captures all aspects of AFOSI investigative work.

Analysis and Reporting Tool] report that field leaders use to identify files within I2MS with missing data (fingerprint cards and final disposition reports). Finally, the Headquarters AFOSI, Inspections Branch (HQ AFOSI/IGI), examines investigative files for compliance with policy, investigative sufficiency, and data integrity.

Recommendations, Management Comments, and Our Response

Recommendation E.1

We recommend that the Secretary of the Air Force take prompt action to:

- a. **Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 12 AFOSI fingerprint cards and 13 AFOSI final disposition reports that are not in the Federal Bureau of Investigation Next Generation Identification database.**
- b. **Immediately perform a comprehensive review of all AFOSI criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**
- c. **Ensure that AFOSI command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in AFOSI IG inspections, and is actually conducted.**
- d. **Conduct a comprehensive review of AFOSI criminal history reporting programs to ensure all applicable agency policy, training, fingerprinting, and final disposition report submission processes are consistent with DoDI 5505.11, and are being implemented.**
- e. **Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**

Air Force Comments

The Air Force, including AFOSI and Air Force Security Forces, reviewed our findings and recommendations. The Air Force agreed with the recommendations.

AFOSI stated that it has already taken steps to identify and obtain missing fingerprint cards and disposition reports and will continue that effort. AFOSI stated that it has instituted a three-tier process for reviewing NCIC indexing compliance at the field, regional, and headquarters leadership levels. This

process requires attaching an NCIC Criminal History Report to the case prior to closure along with leadership notes indicating the report accurately reflects the results of the investigation. According to AFOSI, headquarters reviews will now be conducted prior to case file acceptance for closure. In addition, according to the AFOSI response, in October 2017 the AFOSI IG began inspecting AFOSI criminal indexing data as a special interest item during region unit effectiveness inspections. The AFOSI IG will work with functional managers to establish a permanent inspection checklist related to this area. The AFOSI response stated that AFOSI also reviewed agency policy, training, fingerprinting, and final disposition report submission processes and determined they comply with DoDI 5505.11. Finally, the AFOSI stated that it has initiated action to assess compliance with DNA sample submissions, in accordance with DoDI 5505.14.

Our Response

Comments from the Air Force addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Air Force describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that AFOSI has completed agreed upon corrective actions.

Finding F

Air Force Security Forces

Air Force Security Forces did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 93 of 155 (60 percent) fingerprint cards and 93 of 155 (60 percent) required final disposition reports.

Discussion

Air Force Security Forces and its Investigators typically investigate misdemeanor crimes in the Air Force, such as petty theft, simple assault, and traffic crimes.

The Air Force Security Forces fingerprint card and final disposition report submission and compliance rates are shown in Table 6.

Table 6. Air Force Security Forces Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	155
Fingerprint Cards in NGI	62
Fingerprint Cards Not in NGI	93
Fingerprint Card Noncompliance Rate	60%
Final Disposition Reports in NGI	62
Final Disposition Reports Not in NGI	93
Final Disposition Noncompliance Rate	60%

Source: Service JAGs, FBI CJIS, and Air Force Security Forces Center.

Fingerprint Card Collection Process

The Air Force Security Forces Center (AFSFC) representative, a Law Enforcement Specialist with the AFSFC Police Services Branch, told us that the Air Force Security Forces field personnel collected fingerprints on hardcopy fingerprint cards and the Reports and Analysis section mailed the fingerprint cards to the AFSFC. The AFSFC staff then scanned the fingerprint cards and submitted the fingerprint cards electronically through its booking station to the FBI CJIS.

The AFSFC staff told us AFSFC does not have a mechanism to ensure that field units were submitting all of the fingerprint cards required by DoDI 5505.11.

Air Force Security Forces field units submitted final disposition reports directly to the FBI CJIS, but there was no mechanism to ensure that the field units were submitting all of the final disposition reports required by DoDI 5505.11.

Fingerprint Card Submission Guidance and Training

We reviewed AFSFC fingerprint guidance in Air Force Instruction (AFI) 31-118, “Security Forces Standards and Procedures,” March 5, 2014, Incorporating Change 1, December 2, 2015, and determined it provided guidance that conflicts with DoDI 5505.11. DoDI 5505.11 requires fingerprint card submission upon a probable cause determination for military members investigated for qualifying offenses. However, AFI 31-118 states the reports and analysis section is responsible for fingerprint submission. The reports and analysis section receives the case file with the fingerprint cards at the end of the investigation. This process delays fingerprint card submissions.

We also reviewed AFI 31-120, “Security Forces Systems and Administration,” April 1, 2015, and it states that prosecutors and court officials will submit final disposition reports to the FBI upon final disposition. DoDI 5505.11 requires the LEOs to submit the final disposition report to the FBI CJIS. AFI 31-120 conflicts with DoDI 5505.11 and AFI 31-118.

The AFSFC Police Services Branch has fingerprinting training as a part of its Annual Home-Station Training requirements. Air Force Security Forces unit commanders are responsible to ensure units complete the required fingerprinting training. The AFSFC Police Services Branch also provides fingerprint training to Security Forces non-commissioned officers and commissioned officers at the Security Forces Academy.

We reviewed the AFSFC presentation slides, “Completing a Federal Document (FD) 249/Criminal Fingerprint Card,” and found that the training focused on the collection of fingerprints, but does not address requirements to submit fingerprint cards and final disposition reports to the FBI CJIS.

LEO Oversight

In June 2017, the Air Force Security Forces told us that units use the Management Internal Control Toolset (MICT), which is the Air Force’s centralized repository for inspection checklist and reporting. The Security Forces MICT checklist items are supposed to be monitored and assessed as part of the installation commander’s self-inspection program. Air Force Security Forces is required to conduct self-inspections of its programs and field units using the Security Forces MICT.

The AFI 31-118 Security Forces MICT checklist has a line item to validate whether the fingerprinting procedures are being followed for criminal offenses in accordance with DoDI 5505.11. However, the checklist does not include fingerprint card and final disposition report submission compliance.

We asked the AFSFC representative why Air Force Security Forces fingerprint card and final disposition report submission rates were deficient given the emphasis on training, and the units' oversight compliance checks. The AFSFC representative attributed the compliance deficiency to units being unfamiliar with fingerprint card and final disposition report submission requirements, units not using available training, and the lack of installed software for live scan devices the Air Force purchased.

Recommendations, Management Comments, and Our Response

Recommendation F.1

We recommend that the Secretary of the Air Force take prompt action to:

- a. **Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 93 Air force Security Forces fingerprint cards and 93 Air Force Security Forces final disposition reports that are not on file in the Federal Bureau of Investigation Next Generation Identification database.**
- b. **Immediately perform a comprehensive review of all Air Force Security Forces criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**
- c. **Ensure Air Force Security Forces command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure such compliance is included as a special interest item in future IG inspections, and is actually conducted.**
- d. **Conduct a comprehensive review of Air Force Security Forces criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.**
- e. **Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**
- f. **Direct the Director of Air Force Security Forces to revise AFI 31-120 to align with final disposition report submission requirements set forth in DoDI 5505.11.**

Air Force Comments

The Air Force Security Forces described steps it is taking to implement the recommendations, such as identifying and obtaining missing fingerprint cards and disposition reports. The Air Force Security Forces has initiated an audit of all of their accessible Security Forces case files and will work with the FBI as necessary to resolve discrepancies as possible within the limits of the law. The Air Force Director of Security Forces issued direction in November 2017 for all Security Forces Squadrons to re-accomplish their applicable MICT communicator and to ensure compliance with law and policy. The Air Force Deputy Chief of Staff, Logistics, Engineering, and Force Protection, reiterated this direction to the Major Commands. In addition, the Air Force Security Forces stated that it initiated a policy, process, and training review to ensure they are consistent with DoDI 5505.11. In addition, the Air Force Security Forces has also incorporated other required investigative and criminal history information such as DNA into their on-going policy, process, and training review. The Air Force Security Forces corrected AFI 31-120, and the instruction is in final coordination, with an anticipated official publication in 90 days.

Our Response

Comments from the Air Force addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Air Force describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that Air Force Security Forces has completed agreed upon corrective actions.

Finding G

Marine Corps MP and CID

Marine Corps MP and CID did not consistently submit the required fingerprint cards and final disposition reports. We determined that it failed to submit 37 of 129 (29 percent) required fingerprint cards and 46 of 129 (36 percent) required final disposition reports.

Discussion

The Marine Corps Military Police (MP) and Criminal Investigation Division (CID) (hereafter referred to as the “Marine Corps LEOs”) assigned to the Marine Corps Installations Command typically investigate misdemeanor crimes in the Marine Corps, such as petty theft, simple assault, and traffic crimes.

The Marine Corps LEOs fingerprint card submission data and final disposition report data and compliance rates are shown in Table 7.

Table 7. USMC MP and CID Fingerprint Card and Final Disposition Report Submissions

Description	Submissions
Convicted Offenders	129
Fingerprint Cards in NGI	92
Fingerprint Cards Not in NGI	37
Fingerprint Card Noncompliance Rate	29%
Final Disposition Reports in NGI	83
Final Disposition Reports Not in NGI	46
Final Disposition Noncompliance Rate	36%

Source: Service JAGs, FBI CJIS, NCIS, and USMC LE-CID.

Fingerprint Card Collection Process

According to a United States Marine Corps Law Enforcement CID (USMC LE-CID) staff investigator, Marine Corps LEOs collected fingerprints on hard copy fingerprint cards and mailed the fingerprint cards to NCIS Headquarters for electronic scanning and submission to the FBI CJIS. If NCIS Headquarters rejected a hard copy fingerprint card submission from a field unit, the NCIS notified USMC LE-CID staff of the rejection. The USMC LE-CID staff then directed the field unit to recollect the fingerprints and resubmit the fingerprint card. The NCIS staff keeps a log of rejected fingerprint cards, and checks the status of those it had rejected with field units on a monthly basis.

The NCIS Biometrics Branch Chief stated that his staff scanned fingerprint cards upon receipt from field units, but the NCIS Biometrics Branch did not have a process to ensure field units submitted fingerprint cards for all qualifying convicted offenders as required by DoDI 5505.11. In addition, Marine Corps field units submitted final disposition reports directly to the FBI CJIS, but there was no mechanism to ensure that the field units were submitting all of the final disposition reports required by DoDI 5505.11.

Fingerprint Card Submission Guidance and Training

We reviewed Marine Corps Order 5580.2B, Law Enforcement Manual,” August 27, 2008, and found it did not provide guidance for USMC LEO personnel to take and submit fingerprint cards or submit final disposition reports to the FBI CJIS. However, Marine Corps LEOs were following NCIS guidance for fingerprint card and final disposition report submissions. On December 30, 2015, USMC published Marine Corps Order 5580.2B, with change 2, “Law Enforcement Manual,” which provided updated instructions for fingerprint card and final disposition report submission requirements consistent with both NCIS and DoDI 5505.11 requirements.

Marine Corps CID agents attend the USAMPS CIDSAC and a select group of Marine Corps MPs attend the USAMPS MPI Course. However, the training focused on taking fingerprints solely for evidentiary purposes, but does not teach students the requirement to submit fingerprint cards or final disposition reports to the FBI CJIS.

LEO Oversight

Since 2011, the USMC LE-CID staff had responsibility for the Marine Corps Law Enforcement Accreditation Program, which inspected Military Police Operations on a recurring basis. Compliance with fingerprint card and final disposition report submission requirements was supposed to be part of the inspection process.

We reviewed the results of ten USMC LE-CID inspections. Inspectors found noncompliance at six locations; however, all offices were re-inspected after 6 months and found to be fully compliant by the USMC LE-CID.

On June 12, 2017, the Marine Corps discontinued this program in order to streamline various inspection processes. USMC staff members told us that future Marine Corps LEO assessments, including fingerprint card and final disposition report submissions, will occur during USMC Inspector General Inspections. The Marine Corps message, Subject: “Discontinuation of the Marine Corps Law Enforcement Accreditation Program (MCLEAP),” did not reflect when the Marine Corps IG would start inspecting LEOs.

The USMC LE-CID staff also proactively sent correspondence, beginning in January 2016, to all USMC LEOs identifying the need for additional field supervision over fingerprint card and final disposition report submissions.

We interviewed USMC LE-CID staff, who told us compliance was deficient due to lack of supervision at the patrol, operations, and watch commander levels; difficulty in obtaining disposition data from Commanders or SJAs in order to submit the information to the FBI CJIS as required; and lack of funding to obtain functioning live scan equipment.

The NCIS Biometrics Branch Chief told us he believed the Marine Corps LEOs’ final disposition report submission rates would improve when newer live scan equipment is distributed, because it would allow the submission of final disposition reports directly to the FBI CJIS.

Recommendations, Management Comments, and Our Response

Recommendation G.1

We recommend that the Secretary of the Navy and Commandant of the Marine Corps take prompt action to:

- a. Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 37 fingerprint cards and 46 final disposition reports of the Marine Corps that are not on file in the Federal Bureau of Investigation Next Generation Identification database.**
- b. Immediately perform a comprehensive review of all Marine Corps criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.**

- c. **Ensure Marine Corps command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure such compliance is included as a special interest item in IG inspections and is conducted.**
- d. **Conduct a comprehensive review of Marine Corps criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.**
- e. **Also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.**

Marine Corps Comments

The Marine Corps reviewed our findings and recommendations and agreed with the recommendations. The Marine Corps described steps it is taking to implement the recommendations, such as tasking all installation Provost Marshal's Offices and CID offices to review all incident reporting to determine if suspect fingerprint cards and final disposition reports were completed and submitted to the FBI. In addition, the Marine Corps is reviewing all hard copies of available MP incident reports and CID Reports of Investigation from January 2015 through October 31, 2017 to determine compliance with DoDI 5505.11, and will update its policy to revise the process for oversight control. The Marine Corps also directed its Law Enforcement Branch to review and revise the Marine Corps Law Enforcement Training and Readiness Manual to ensure full compliance with DoDI 5505.11, in addition to updating the training standards for both the MP Basic Course and the CP Basic Officer Course. Finally, the Marine Corps will update associated IG checklists for both MP and CID to ensure that DNA is collected, processed, and submitted for inclusion in FBI databases.

Our Response

Comments from the Marine Corps addressed the intent of the recommendations. Therefore, the recommendations are resolved. We request regular updates from the Marine Corps describing its progress in implementing the recommendations and the steps it stated it would take in response to the recommendations. We will consider these recommendations formally closed after we verify that the Marine Corps has completed agreed upon corrective actions.

Additional Recommendations to Other DoD Components

Recommendations, Management Comments, and Our Response

Recommendation H.1

We recommend that the Under Secretary of Defense for Intelligence and the Deputy Chief Management Officer ensure that the Directors of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency, and the Pentagon Force Protection Agency take prompt action to:

- a. Immediately perform a comprehensive review of all their criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.
- b. Ensure that supervisory and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is regularly inspected.
- c. Conduct a comprehensive review of their criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.
- d. Also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence agreed with our recommendations. In addition, the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) described steps it is taking to implement the recommendations. The OUSD(I) told us it will engage with the noted Defense Intelligence Components to validate their collection and reporting of fingerprint records and final disposition reports, and ensure that appropriate policies and controls exist in this regard and are consistent with DoDI 5505.11. The OUSD(I) said it will report the findings of this review, and any noted corrective actions, to DoD IG upon completion.

Our Response

Comments from the OUSD(I) addressed the intent of the recommendations. Therefore the recommendations are resolved. We request regular updates from the OUSD(I) describing the Defense Intelligence Components' progress in implementing the recommendations. We will consider these recommendations formally closed after we verify that the Defense Intelligence Components have completed agreed upon corrective actions.

Chief Deputy Management Officer Comments

The Deputy Chief Management Officer agreed with the recommendations. In addition, the DCMO described steps it is taking to implement the recommendations. The Pentagon Force Protection Agency (PFPA) will conduct a comprehensive review to ensure all fingerprint cards and final disposition reports have been reported in compliance with the DoD and FBI requirements. PFPA will review its policy, training, processes, and oversight controls to ensure compliance with DoDI 5505.11 and take corrective actions by March 1, 2018. PFPA will also ensure that other required investigative and criminal information is submitted for inclusion in the FBI databases. In addition, the DCMO stated that PFPA is working with the Defense Management Data Center to develop a process to report information to the Defense Incident-Based Reporting System. PFPA expects to have a solution by March 1, 2018. PFPA is also finalizing guidance to ensure the proper collection of DNA samples from suspects of criminal investigations, expecting publication and implementation by February 1, 2018.

Our Response

Comments from the DCMO addressed the intent of the recommendations. Therefore the recommendations are resolved. We request regular updates from the DCMO describing its progress in implementing the recommendations. We will consider these recommendations formally closed after we verify that Pentagon Force Protection Agency has completed agreed upon corrective actions.

Additional Management Comments

The Defense Criminal Investigative Service (DCIS), the criminal investigative component of the DoD OIG, agreed with the recommendations and also provided comments outlining actions it is taking to ensure it has submitted all required investigative and criminal history data for inclusion in FBI databases.

Specifically, DCIS has initiated a comprehensive examination of all closed investigations, which will ultimately go back to 1998, to determine if it complied with its reporting requirements. DCIS also directed a policy review to ensure its compliance with requirements conveyed in DoDI 5505.11. Additionally, DCIS will update case closure checklists to require mandatory validation of information submitted to the FBI. DCIS will also include validation of this information as a special interest item on future inspections of DCIS operations and will institute periodic spot checks of closed cases to evaluate the agency's validation requirements.

Overall Conclusions

This evaluation assessed whether the Military Services had submitted required fingerprint cards and final disposition reports in 2015 and 2016 for their service members who were convicted of qualifying offenses. We previously conducted two other evaluations, in 1997 and 2015, that found a significant number of missing fingerprint cards and final disposition reports throughout the DoD.

In the current evaluation, we again identified many missing fingerprint cards and final disposition reports throughout the DoD. Overall, of the 2,502 fingerprint cards required to be submitted, we identified 601 (24 percent) that were missing. Of 2,502 required final disposition reports required to be submitted, 780 (31 percent) were missing.

Within the Services, the Army, Navy, and the Marine Corps had more missing fingerprint cards and final disposition reports. The Army had 262 (28 percent) missing fingerprint cards and 385 (41 percent) missing final disposition reports. The Navy had 197 (29 percent) missing fingerprint cards and 243 (36 percent) missing final disposition reports. The Marine Corps had 37 (29 percent) missing fingerprint cards and 46 (36 percent) missing final disposition reports.

The Air Force had fewer missing fingerprint cards and disposition reports, although many were still missing. In the Air Force, we identified 105 (14 percent) missing fingerprint cards and 106 (14 percent) missing final disposition reports.

Any missing fingerprint card and final disposition report can have serious, even tragic, consequences, as may have occurred in the recent church shooting in Texas. The failure to populate FBI databases with all the required fingerprint records can result in someone purchasing a weapon who should not. It can also hinder criminal investigations and potentially impact law enforcement and national security interests.

It is therefore troubling that many fingerprint cards remained missing. In this evaluation, we did not determine the exact causes for the deficient practices among the Services, who did not ensure that the required records were submitted. We recently announced a related evaluation to this one, which will examine the policies, practices, and procedures regarding the submission of required information to FBI databases. That evaluation will also assess the causes for the enduring deficiencies that we found in this review.

However, we believe that Military Services, from the top leadership on down, need to focus attention on this issue immediately and ensure that required information is submitted to FBI databases. We therefore make specific recommendations to all the Services to ensure that the fingerprint cards and disposition reports that we identified as missing are submitted. We also recommend that the Services perform a comprehensive review, to ensure that required fingerprint cards and disposition reports have been submitted. We recommend that this comprehensive review go back at least to 1998, when the first DoD Instruction was issued that required all DCIOs and LEOs to collect and submit fingerprint cards and final disposition reports to the FBI CJIS.

We recognize that due to the passage of time, some cards and disposition reports may not be able to be obtained or submitted for all violations that require such submissions. However, because of the impact that any missing card can have, we recommend that the Services conduct comprehensive reviews to ensure that all additional information that can be submitted is, in fact, submitted.

We recommend that the comprehensive reviews should also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

In addition, we recommend that the Services take prompt action to institute command, supervisory, and management oversight controls to verify compliance with fingerprint card and final disposition report submission requirements, in the past and in the future. In particular, we recommend that the Services also ensure that such compliance is included as a special interest item in Service Inspector General inspections.

In determining what controls and processes are needed to ensure the required submissions are made, we believe the Services should consider some potential best practices identified in this report, such as more widely using live scan equipment to capture fingerprints, which can help prevent inked fingerprint cards from being rejected because of poor quality; requiring supervisory certification of the required submission before a case can be closed; mandating specific training on collecting and submitting fingerprint cards and final disposition reports to the FBI; and requiring in the case management database a completed field showing that fingerprint cards and final disposition reports have been submitted before the case can be closed in the database.

While this evaluation did not examine the compliance of all other DoD law enforcement organizations, such as the Pentagon Force Protection Agency (PFPA), the National Security Agency police, and other law enforcement organizations within DoD components, we believe that they also must ensure that all fingerprints, final disposition reports, and other required investigative and criminal history information has been submitted to the FBI, as required by DoD policy.²⁰ We therefore included another recommendation addressed to DoD law enforcement components to ensure that all required information is submitted to the FBI.

In response to the draft report, the Military Services and the other DoD law enforcement components agreed with the recommendations and outlined steps they are taking and will take to fully implement the recommendations. These comments were responsive to the recommendations. However, we have requested regular updates from the DoD components regarding their progress in implementing the recommendations.

Finally, the DoD OIG recently announced that we will conduct another review to assess the policies, practices, and procedures for submitting criminal history information to the FBI. This review will also examine the implementation of corrective actions and whether there are best practices for ensuring submission of criminal history information that should be adopted throughout the DoD. However, given the serious consequences that can result from deficient practices and any missing information we believe the Services and the DoD law enforcement organizations should not wait for those recommendations to continue to fix this urgent problem. The Services and the law enforcement organizations should work diligently to immediately ensure that all required investigative and criminal history information has been submitted for inclusion in FBI databases.

²⁰ The DoD OIG is currently completing a broader evaluation of PFPA's criminal investigative practices, including submission of required fingerprints, final disposition reports, and other criminal history information to the FBI.

Appendix A

Scope and Methodology

We conducted this evaluation from February 2017 through October 2017. We conducted the evaluation in accordance with the “Quality Standards for Inspection and Evaluation” published by the Council of the Inspectors General on Integrity and Efficiency in January 2012. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our review.

DoDI 5505.11 requires that fingerprint cards be submitted on all Military Service members investigated by a DoD LEO when probable cause exists to believe that the person has committed a [qualifying offense listed in this instruction], following coordination with the . . . servicing SJA or legal advisor. DoDI 5505.11 also requires final disposition report submission once action is taken. Our evaluation focused on fingerprint card and final disposition report submissions for Military Service members convicted of qualifying offenses.

We asked the Military Services’ Judge Advocate Generals (JAG) and the Staff Judge Advocate to the Commandant of the Marine Corps, for records of Military Service members convicted between January 1, 2015, and December 31, 2016 of qualifying offenses listed in Enclosure 2 of DoDI 5505.11. Based on the information provided by the JAGs, we identified a total of 2,502 Military Service members who were convicted by court-martial of qualifying offenses during our evaluation period. We then identified the Military Service LEO that conducted the investigation for each conviction requiring the submission of fingerprint cards and final disposition reports to the FBI CJIS for entry into the FBI NGI database.

We submitted the identifying information associated with the convicted offenders to the FBI CJIS, which led to the development of a list of convicted offenders who did not have fingerprint cards or final disposition reports on file in the FBI NGI database.²¹ Next, we sent that list to the LEOs for validation and requested supporting documentation and justifications for the name of convicted offenders who did not have fingerprint cards or final disposition reports on file in the FBI NGI database.²²

²¹ Our submission rate calculations are based on LEO input as of July 28, 2017.

²² Disposition information can be submitted on fingerprint cards or on final disposition reports. Our final disposition report numbers include both types of submissions.

Throughout this evaluation, Service JAG representatives provided us information about offender court-martial convictions and identified investigating organizations. LEO representatives provided us the following information pertaining to their respective organization:

- guidance applicable to fingerprinting subjects and oversight of fingerprint card and final disposition report submission processes,
- investigative case information, such as case numbers, date initiated, investigating organization, FBI Numbers, TCNs, and the rationale for non-submission of fingerprint cards and final disposition reports,
- training related to fingerprint card and final disposition report submissions, and
- inspection procedures and results.

We also reviewed policy and guidance documents, inspection reports, and training materials; interviewed Military Service LEO subject matter experts; and visited LEO field offices for each Military Service.

Use of Computer-Processed Data

We used computer-processed data to perform this evaluation.

Each of the Service JAGs populated our spreadsheet with information retrieved from the respective military justice systems below. We did not verify the reliability of the Service JAGs data.

- Army Courts-Martial Information System (ACMIS)
- Navy and Marine Corps Case Management System (CMS)
- Air Force Automated Military Justice Administration and Management System (AMJAMS)

Each of the military LEOs used its respective reporting systems to retrieve information about the convicted offenders identified by the JAGs. We did not verify the reliability of the LEO's data.

- Law Enforcement Defense Data Exchange (D-DEx)
- Army Law Enforcement Reporting and Tracking System (ALERTS)
- Navy Consolidated Law Enforcement Operations Center (CLEOC)
- Air Force Investigative Information Management System (I2MS)
- Security Forces Management Information System (SFMIS)

The FBI CJIS used its data storage and reporting systems to validate information submitted by the LEOs about convicted offenders identified by the Service JAGs. We did not verify the reliability of the FBI CJIS data.

- FBI National Criminal Information Center (NCIC)
- Integrated Automated Fingerprint Identification System (IAFIS)
- Next Generation Identification (NGI)

Appendix B

Qualifying Offenses

DoDI 5505.11 Enclosure 2 Qualifying Offenses

Article	Offense Description
78	Accessory after the fact (for crimes listed in this enclosure)
80	Attempts (for crimes listed in this enclosure)
81	Conspiracy (for crimes listed in this enclosure)
82	Solicitation
85	Desertion
90	Striking or assaulting a superior commissioned officer
91	Striking or assaulting a warrant, noncommissioned, or petty officer
94	Mutiny and sedition
95	Resistance, flight, breach of arrest, and escape
97	Unlawful detention
106	Spies
106a	Espionage
107	False official statements
108	Military property of the United States – sale, loss, damage, destruction, or wrongful disposition
109	Property other than military property of the United States – waste, spoilage, or destruction
111	Drunken or reckless operation of vehicle, aircraft, or vessel
112a	Wrongful use, possession, etc., of controlled substances
116	Riot or breach of peace
118	Murder
119	Manslaughter
119a	Death or injury of an unborn child
120	Rape and carnal knowledge for offenses committed on or after June 28, 2012
120	Rape, sexual assault, and other sexual misconduct for offenses committed on or between October 1, 2007, and June 27, 2012
120	Rape and carnal knowledge for offenses committed before October 1, 2007
120a	Stalking
120b	Rape and sexual assault of a child for offenses committed on or after June 28, 2012
120c	Other sexual misconduct of offenses committed on or after June 28, 2012
121	Larceny and wrongful appropriation

DoDI 5505.11 Enclosure 2 Qualifying Offenses (cont'd)

Article	Offense Description
122	Robbery
123	Forgery
123a	Making, drawing, or uttering check, draft, or order without sufficient funds
124	Maiming
125	Forcible sodomy; bestiality, in accordance with section 1707 of Public Law 113-66 (Reference h)), which repealed the offense of consensual sodomy under the UCMJ
126	Arson
127	Extortion
128	Assault
129	Burglary
130	Housebreaking
131	Perjury
132	Frauds against the United States
134a.	Assault – Indecent for offenses committed before October 1, 2007
b.	Assault – with intent to commit murder, voluntary manslaughter, rape, robbery, sodomy, arson, burglary, or housebreaking
c.	Bribery and graft
d.	Burning with intent to defraud
e.	Child endangerment for offenses committed on or after October 1, 2007
f.	Child pornography offenses, to include possession, distribution, production, receipt, viewing, and accessing
g.	Correctional custody – offense against
h.	False or unauthorized pass offenses
i.	Obtaining services under false pretenses
j.	False swearing
k.	Willfully discharging a firearm under such circumstances as to endanger human life
l.	Fleeing the scene of an accident
m.	Negligent homicide
n.	Impersonating a commissioned, warrant, noncommissioned, or petty officer, or an agent or official
o.	Indecent acts or liberties with a child for offenses committed prior to October 1, 2007
p.	Indecent exposure for offenses committed before October 1, 2007
q.	Indecent language
r.	Indecent acts with another for offenses committed before October 1, 2007

DoDI 5505.11 Enclosure 2 Qualifying Offenses (cont'd)

Article	Offense Description
s.	Kidnapping
t.	Taking, opening, secreting, destroying, or stealing mail
u.	Depositing, or causing to be deposited, obscene matters in mail
v.	Misprision of serious offense
w.	Obstructing justice
x.	Wrongful interference with an adverse administrative proceeding
y.	Pandering and prostitution. Having someone commit an act of prostitution is still an offense pursuant to Article 134 of the UCMJ, but if the pandering is "compelled," it becomes an Article 120 offense, on or between October 1, 2007 and June 27, 2012, and Article 120c offense on or after June 28, 2012
z.	Subornation of perjury
aa.	Altering, concealing, removing, mutilating, obliterating, or destroying public records
ab.	Reckless endangerment
ac.	Destruction, removal, or disposal of property to prevent seizure
ad.	Self-injury without intent to avoid service
ae.	Soliciting another to commit an offense (for crimes listed in this enclosure)
af.	Knowingly receiving, buying, or concealing stolen property
ag.	Wrongful refusal to testify
ah.	Threat or hoax designed or intended to cause panic or public fear
ai.	Communicating threat
aj.	Wrongfully concealing or carrying a weapon
ak.	Specific federal statutes charged as a violation of Article 134 of the UCMJ: (1) Aggravated identity theft (2) Fraud and related activity in connection with computers (3) Fraud and related activity in connection with identification documents, authentication features, and information (4) Sabotage
al.	Any state criminal offenses pursuant to section 13, title 18, United States Code (18 U.S.C. § 13) (also known as the "Federal Assimilative Crimes Act"), charged as a violation of Article 134 of the UCMJ

Appendix C

Prior Coverage

The Department of Defense Inspector General (DoD IG) previously issued several reports related to fingerprint card and disposition data submission.

Report No. DoDIG-2015-081, “Evaluation of Department of Defense Compliance with Criminal History Data Reporting Requirements,” February 12, 2015

This DoD OIG evaluation examined whether DoD Military Criminal Investigative Organizations (MCIOs) and other DoD law enforcement organizations reported offender criminal history data collected from service members convicted of qualifying offenses between June 1, 2010, and October 31, 2012, and submitted the data to the Federal Bureau of Investigation’s (FBI) Criminal Justice Information Services (CJIS) Division as DoD policy mandates.

Specifically, the DoD OIG determined whether fingerprints and final disposition reports for 1,102 Navy, Air Force, and Marine Corps service members convicted of qualifying offenses were submitted to the FBI CJIS. Our analysis did not determine the reasons that fingerprints or final disposition reports that should have been included in IAFIS were not. We determined that the Navy failed to submit 68 of 317 (21 percent) required fingerprint cards and 80 of 317 (25 percent) required disposition reports. The Air Force failed to submit 110 of 358 (31 percent) required fingerprint cards and 113 of 358 (32 percent) required disposition reports and the Marine Corps failed to submit 126 of 427 (30 percent) required fingerprint cards and 141 of 427 (33 percent) required final disposition reports

We recommended that the Secretaries of the Navy and Air Force take prompt action to submit the missing fingerprints and final disposition reports to the FBI for inclusion into IAFIS.

In addition, we recommended that the Secretaries of the Navy and Air Force take prompt action to ensure fingerprints and final disposition reports for future arrestees and convicted offenders conform to DoD Instruction 5505.11, “Fingerprint Card and Final Disposition Report Submission Requirements.”

The Secretaries of the Navy and Air Force agreed with our recommendations but expressed concern regarding their jurisdictional and legal authority to collect criminal history data from individuals no longer subject to the Uniform Code of Military Justice.

Report No. PO 97-003, "Criminal Investigations Policy Memorandum Number 10, Criminal History Data Reporting Requirements," January 28, 1997

This evaluation was performed as a result of a requirement in the "National Defense Authorization Act for Fiscal Year 1996." The Secretary of Defense was directed to provide a report to Congress on the consistency with which fingerprint cards and final dispositions are reported by the DCIOs to the FBI for inclusion in the Bureau's criminal history identification files.

The DoD OIG evaluation's primary objective was to examine whether the DCIOs were reporting fingerprint cards and final disposition reports to the FBI in compliance with DoD Criminal Investigations Policy Memorandum Number 10 (CPM No. 10), Criminal History Data Reporting Requirements, March 25, 1987.

The DoD OIG determined that the MCIOs were not consistently submitting criminal history data to the FBI criminal history files. Specifically, the evaluation determined that between December 1995 and July 1996, the Army failed to send fingerprint cards to the FBI in approximately 82 percent of the cases; the Navy 83 percent; and the Air Force 38 percent. Failure to submit the final disposition report, in the Army was 79 percent; the Navy 94 percent; and the Air Force 50 percent.

The DoD OIG determined that the level of the MCIOs' noncompliance in the submission of fingerprint cards and final dispositions was high and consistent throughout the MCIOs. Inadequate implementing procedures, lack of emphasis by the MCIOs on reporting, and lack of sufficient oversight focusing on this issue contributed significantly to the noncompliance. The DoD OIG further found that definitive and comprehensive guidance with management emphasis was needed at all levels to improve reporting.

The primary objective of the 1997 evaluation focused on the MCIOs' compliance with reporting criminal history data. In addition, the evaluation determined that other Service law enforcement organizations, such as the Army Military Police, Navy and Air Force Security Police (now Security Forces), and Marine Corps Criminal Investigation Division CID (Marine Corps CID), and Defense Agencies with law enforcement organizations, did not consistently report the criminal history data as required.

The report recommended that Military Departments and Defense Agencies law enforcement organizations investigating serious offenses as described in CPM No. 10 develop interim policies and implementing procedures for reporting to the FBI criminal history data files while awaiting a new DoD Instruction.

The Army concurred with the recommendation and stated that policy guidance would be established requiring the submission of reporting documents within 10 working days of a triggering event. The Army also stated that compliance on reporting requirements would be an inspected item during assistance visits to all field units.

The Navy disagreed with the finding, stating that statistical data are questionable because an FBI backlog in data entry exists and the requirements for the use of plain language on the FD-249 may have resulted in the FBI not processing submissions. In addition, the Navy did not agree with the recommendation, stating that NCIS had policy and implementing procedures already in place that adequately address CPM No. 10 and reflect the guidance of the IG, DoD, memorandum, November 14, 1996.

The Air Force concurred with the recommendation and stated that procedural guidance in the DoD OIG memorandum of November 14, 1996, would be used until a new DoD Instruction was developed. The AFOSI issued a memorandum on December 9, 1996, informing its field units of the suggested DoD OIG policy and emphasized that reporting requirements are a mandatory inspection item for all AFOSI self-inspections and AFOSI Inspector General inspections. In addition to these two evaluations, the DoD OIG has issued several other reports that include information on the Military Services' submission of criminal history data to the FBI for inclusion in its criminal history databases.

In addition to these two evaluations, the DoD OIG has issued several other reports that include information on the Military Services' submission of criminal history data to the FBI for inclusion in its criminal history databases.

Report No. DoDIG-2017-054, "Evaluation of Military Criminal Investigative Organizations' Adult Sexual Assault Investigations," February 14, 2017

The DoD OIG evaluated a sample of 376 Army, Navy, Air Force, and Marine Corps subjects who were investigated for sexual assault between January 1, 2014 and December 31, 2015, and were required to have their fingerprints collected and submitted to the FBI CJIS. The DoD OIG determined that 15 of 376 (4 percent) fingerprint cards were not collected by MCIOs or were collected but not submitted to the FBI. The MCIO's had an overall fingerprint collection noncompliance rate of 4 percent.

Report No. DoDIG-2015-094, "Evaluation of Military Criminal Investigative Adult Sexual Assault Investigations," March 24, 2015

The DoD OIG evaluated a sample of 532 Army, Navy, Air Force, and Marine Corps subjects who were investigated for sexual assault between January 1, 2012 and December 31, 2013, and were required to have their fingerprints collected and submitted to the FBI CJIS. The DoD OIG determined that 51 of 532 (10 percent) fingerprint cards were not collected by MCIOs, or were collected but not submitted to the FBI CJIS. The MCIOs had an overall fingerprint collection noncompliance rate of 10 percent.

Report No. DoDIG-2015-055, "Evaluation of Military Criminal Investigative Organizations' Child Death Investigations," December 22, 2014

The DoD OIG evaluated a sample of 82 Army, Navy, Air Force, and Marine Corps Service members who were subjects in child death investigations between October 1, 2012 and September 30, 2013, and were required to have their fingerprints collected and submitted to the FBI CJIS. The DoD OIG determined that 2 of 82 (2 percent) fingerprints were not collected by MCIOs or were collected but were not submitted to the FBI CJIS. The MCIOs had an overall fingerprint collection noncompliance rate of 2 percent.

Report No. DoDIG-2015-011, "Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting and Reporting Accuracy," October 29, 2014

The DoD OIG evaluated the Defense Criminal Investigative Organizations' (DCIOs) process for reporting accurate criminal incident data to Defense Incident-Based Reporting System (DIBRS) in accordance with DoD Manual (DoDM) 7730.47-M, Volume 1, "Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements," December 7, 2010. The FBI uses this data to develop a reliable set of criminal statistics for U.S. law enforcement agencies.

The DoD OIG determined that the DoD was not reporting criminal incident data to the FBI for inclusion in the annual Uniform Crime Reports to the President, the Congress, State governments, and officials of localities and institutions participating in the Uniform Crime Report Program, as required by Federal law.

This evaluation also determined that the DoD had not completed the FBI's requirements for the DIBRS database certification; therefore the DoD did not report criminal incident data to the Attorney General, through the FBI, for inclusion in the Uniform Crime Report, as required by the Uniform Federal

Crime Reporting Act of 1988 and DoD Directive 7730.47. For approximately 10 years, since the DIBRS database became operational, DIBRS has functioned as a database that did not populate its data into NIBRS for inclusion in the Uniform Crime Report.

The evaluation reported that although the DoD is a Federal agency that routinely investigates complaints of criminal activity, it does not report details about such crimes to the FBI for inclusion in the National Incident-Based Reporting System database and the annual uniform crime reports. The DIBRS Database Administrator was aware of the FBI's requirements to obtain certification, but had not submitted the required DoD criminal incident data to NIBRS to obtain the certification. As a result, DMDC has never submitted DIBRS data to the FBI for inclusion in their annual UCRs.

Report No. DoDIG-2014-105, "Evaluation of Military Criminal Investigative Organizations' Child Sexual Assault Investigations," September 9, 2014

The DoD OIG evaluated a sample of 153 Army, Navy, Air Force, and Marine Corps subjects who were investigated for the sexual assault of children between April 2013 and July 2013, and were required to have their fingerprints collected and submitted to the FBI CJIS. The DoD OIG determined that 24 of 153 (16 percent) fingerprints were not collected by MCIOs, or were collected but were not submitted to the FBI CJIS. The MCIOs had an overall fingerprint card collection noncompliance rate of 16 percent.

Report No. DoDIG-2014-029, "Review of Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations," February 27, 2014

The DoD OIG evaluated whether the Military Services law enforcement and confinement authorities collected DNA samples from service members convicted of qualifying offenses between June 1, 2010 and October 31, 2012, and submitted those samples to U.S. Army Criminal Investigation Laboratory (USACIL) for analysis and inclusion into the Combined DNA Index System (CODIS). The DoD OIG determined that the DoD did not submit 279 of the 3,490 (8 percent) (excludes U.S. Coast Guard submissions) required DNA samples to USACIL for inclusion in CODIS during our evaluation sample period of June 1, 2010, through October 31, 2012. The evaluated agencies had an overall fingerprint collection noncompliance rate of 8 percent.

Report No. DoDIG-2013-091, "Evaluation of Military Criminal Investigative Organizations' Sexual Assault Investigations," July 9, 2013

The DoD OIG evaluated a sample of 501 Army, Navy, Air Force, and Marine Corps sexual assault subjects identified in investigation reports that closed out in 2010, and were required to have their fingerprints collected and submitted to the FBI for inclusion in the IAFIS criminal history database. The DoD OIG determined that 101 of 501 (20 percent) fingerprints were not collected by MCIOs, or were collected but were not submitted to the FBI. The MCIOs had an overall fingerprint collection noncompliance rate of 20 percent.

Appendix D

Management Comments

Secretary of the Army



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY
MANPOWER AND RESERVE AFFAIRS
111 ARMY PENTAGON
WASHINGTON, DC 20310-0111

29 NOV 2017

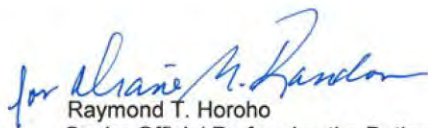
SAMR

MEMORANDUM FOR Inspector General, Department of Defense (Attention: Mr. Jeff Bennett, Oversight Director), 4800 Mark Center Drive, Alexandria, VA 22350-1500.

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Services Law Enforcement Organizations (project No. 2017C002).

1. Reference: Department of Defense Inspector General Project No. 2017C002, Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Services Law Enforcement Organizations, dated 20 November 2017.
2. Please accept the enclosed as the Army's initial response and recommendations to the subject report.
3. POC for this action is Mr. Thomas Blair, Chief of the Law Enforcement Division, Office of the Provost Marshal General at (703) 695-8823 or Thomas.s.blair4.civ@mail.mil.

Encl


Raymond T. Horoho
Senior Official Performing the Duties of the
Assistant Secretary of the Army
(Manpower and Reserve Affairs)

Secretary of the Army (cont'd)



DEPARTMENT OF THE ARMY
Office of the Provost Marshal General
2800 Army Pentagon
Washington, DC 20310-2800

DAPM

28 November 2017

MEMORANDUM FOR Inspector General, Department of Defense (Attention: Ms. Melvina Coakley), 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Services Law Enforcement Organizations (Project No. 2017C002)

1. Reference your 20 November 2017 memorandum, subject as above.
2. Thank you for the opportunity to provide comments to the draft report. I acknowledge your detailed review of fingerprint submissions to the Federal Bureau of Investigation (FBI) and instances of non-compliance by Army law enforcement in submitting fingerprint cards and final disposition cards.
3. The Office of the Provost Marshal General (OPMG) is actively pursuing resolution of the issues identified in the draft report to address the policy, resourcing and manning challenges that led to our current condition. Over the last two weeks, the US Army Criminal Investigation Command (CID) has coordinated with officials at both the National Crime Information Center (NCIC) and the National Instant Criminal Background Check System (NICS) to allow for the submission of automated data regarding felony convictions, drug offenders, convicted domestic violence offenders, and the final disposition for all persons who have fingerprint cards submitted. The CID has also submitted automated final disposition information to NCIC on 4,340 suspects (both CID and installation law enforcement suspects) whose fingerprints were in the system with no final disposition being listed. Additionally, CID has submitted automated information on 19,890 individuals with felony convictions (from 1989 to 2016), 6,386 drug offenders, and 189 individuals convicted of domestic violence to NICS in order to preclude those individuals from purchasing a firearm or explosives. Additionally, 5,215 dishonorable discharges for Army individuals from 1989 to present were previously entered into NICS, and weekly updated information will be provided. Finally, we are working closely with affected Army commands to ensure monthly checks are conducted to ensure submission of fingerprint cards and final disposition reports in accordance with applicable regulations.
4. We reviewed the draft report and recommend the following changes under Finding B:
 - a. Finding B is titled "Army Installation Management Command Military Police." We recommend changing the title to "Army Military Police" to ensure all installation law enforcement-owning commands are included in our efforts to achieve full resolution and compliance. OPMG acknowledges that the review focused on Installation Management

Secretary of the Army (cont'd)

DAPM

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Services Law Enforcement Organizations (Project No. 2017C002)

Command (IMCOM) and that they are the higher headquarters for the preponderance of Army installations. Therefore, we recommend the "Discussion" paragraph be worded to reflect the sentiment that while IMCOM was the focus of the assessment, all Army installation-owning commands should be included in efforts to identify and remedy issues proposed for action as a result of the assessment.

b. Under Finding B, "Fingerprint Card Submission Guidance and Training" (page 12), the draft report references the 2007 version of Army Regulation (AR) 190-45. The OPMG published an update to the regulation on 27 September 2016. OPMG acknowledges that the revision was published late in the period reviewed in this assessment, but requests that the updated revision be acknowledged as well. Additional details follow in paragraph 5.f. below.

c. The footnote under Finding B (page 12), states that the Picatinny Arsenal, NJ, MP station developed electronic submission capability. IMCOM verified that this is incorrect as they are mailing their fingerprint cards to the Crime Records Center (CRC).

d. Under Finding B, "LEO Oversight", paragraph 3 (page 13), we recommend deleting the statement, "However, the absence of live scan technology does not excuse IMCOM units' failure to collect and submit hard-copy fingerprint cards and final disposition reports to USARC for eventual entry into FBI CJIS." This comment is inconsistent with the other services and appears to be unnecessary to state.

5. The OPMG reviewed recommendations in Findings A.1. and B.1. in coordination with CID and IMCOM. As both sets of recommendations are essentially identical, feedback on both lists are consolidated below, with clarification provided as appropriate:

a. Recommendation a: OPMG concurs with this recommendation and, as indicated in paragraph 3 above, we are actively reviewing data and submitting final disposition reports as quickly as possible. OPMG is working with affected Army commands to identify and address resourcing needs for submission of automated fingerprint cards via LiveScan technology. The projected timeline for completion of this effort for the Army is no later than 3rd Quarter of Fiscal Year 2018.

b. Recommendation b: OPMG concurs, with comment, to this recommendation. OPMG is spearheading a review of the Army's law enforcement database to ensure, where possible, missing fingerprint cards and final disposition reports are reported to the FBI in compliance with statutory DoD and FBI requirements. One point of clarification must be made: IMCOM does not own criminal investigative databases, their reports feed into the Army Law Enforcement Reporting and Tracking System (ALERTS). We recommend changing B.1.b. by replacing the word "IMCOM" with "installation;" doing so will ensure all Army commands with responsibility for installation law enforcement are captured in this requirement.

Secretary of the Army (cont'd)

DAPM

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Services Law Enforcement Organizations (Project No. 2017C002)

c. Recommendation c: OPMG concurs with this recommendation. We will ensure that our CID IG continues to assess compliance with fingerprint card and final disposition report requirements. Additionally, our new Army Law Enforcement Compliance Program will assess these areas, which will supplement the monthly compliance checks that we are instituting immediately in accordance with senior Army leadership guidance.


d. Recommendation d: OPMG concurs with this recommendation. OPMG and CID are currently developing a tracking system that compares offenders in ALERTS against fingerprint cards and final disposition reports submitted via LiveScan, Army-wide. Our aforementioned review will also identify and address gaps and shortcomings in policy, resources and manning to ensure fingerprint card/final disposition report submissions.

e. Recommendation e: OPMG concurs with this recommendation. The OPMG-led review will also address shortfalls identified in the submission of DNA to Federal databases.

f. Recommendation 1.B.f: OPMG concurs, with comment, to this recommendation. As mentioned in paragraph 4.b. above, OPMG published an update to the regulation on 27 September 2017. This update states, in paragraph 4-9a, that fingerprint cards should be submitted when a probable cause has been determined. We concur that AR 190-45 needs to be updated to clearly define process and procedures for submitting fingerprint cards. We recently began revising AR 190-45 and will include that update in the revision. A publication date is difficult to define due to the ongoing Regulatory Reform Task Force review, as well as Code of Federal Regulations procedural review requirements; however, we are hopeful that we will publish the revision in Fiscal Year 2019.

6. Again, we appreciate the opportunity to provide feedback on the draft report and look forward to continuing to work together toward successful resolution of the challenges to these important components of our law enforcement programs.

7. Point of contact for this memorandum is the Chief of the Law Enforcement Division, Mr. Thomas S. Blair at 703-695-8823 or thomas.s.blair4.civ@mail.mil.



DAVID P. GLASER
Major General, USA
Provost Marshal General

Secretary of the Navy



THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

November 29, 2017

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by
Military Service Law Enforcement Organizations

This memorandum provides comments on recommendations pertaining to whether all Military Services' Law Enforcement Organizations had submitted fingerprint cards and final disposition reports for Military Service members convicted by courts-martial for qualifying offenses as required by DoD Instruction. The attached is provided by the Department of the Navy.

My point of contact for this action is Mr. Samuel G. Worth, Deputy Director, Navy Criminal Investigative Service, at (571) 305-9000, email samuel.g.worth@ncis.navy.mil.

A handwritten signature in blue ink, which appears to read "R. Spencer", is positioned above the printed name.

Richard V. Spencer

Attachment:
As stated

Secretary of the Navy NCIS



DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

ACTION MEMO

November 28, 2017

FOR: SECRETARY OF THE NAVY

FROM: Samuel G. Worth, Deputy Director

SUBJECT: Evaluation of Fingerprint Card and Final Disposition Report Submissions by
Military Service Law Enforcement Organizations

- NCIS assigned as lead action office for DON with coordination from OGC, DNS, DMCS, NAVIG, OJAG, and DUSN (P). DoD IG requests the Service Secretaries provide comments (TAB A) in response to the DoD IG Draft Report (TAB B) evaluation to determine whether all Military Services' Law Enforcement Organizations (LEOs) had submitted fingerprint cards and final disposition reports for Military Service members convicted by court-martial of qualifying offenses, as required by DoD instruction.
- NCIS was required to respond to the recommendations in section C.1 of the report. NCIS concurs with the recommendations with comments and questions contained in TAB B. NCIS has implemented a plan to correct previous fingerprint submission deficiencies and to prevent further issues with submissions in the future. NCIS' Fingerprint Verification Plan is listed below:
 - Each field office will review all case files currently in their possession (open cases, cases closed within last 12 months, and cases in extended retention) to verify fingerprints have been taken and submitted as required. Field offices will take corrective actions when necessary. Estimated date of completion: Review completed/corrections in progress.
 - NCIS Headquarters, Criminal Investigation Directorate will validate each field office submission and remit any cases requiring corrective action back to the field office for completion. Estimated date of completion: December 8, 2017.
 - NCIS Headquarters will query all case files from January 1, 1998 to September 30, 2016 (historical cases) to determine which have fingerprints already submitted to NCIC. The list of cases with prints already submitted will be reviewed to determine which are missing final disposition.

Secretary of the Navy

NCIS (cont'd)

Estimated date of completion: To date, 691 cases have been reviewed covering periods 2000-2014. The remaining will be completed by December 8, 2017.

- Each of the remaining historical cases from the January 1, 1998 to September 30, 2016 above will be reviewed to determine cases in which command took any level of punitive action and no fingerprints were submitted. The following corrective actions will be attempted:
 - Query case file to determine existence of fingerprint card.
 - Ascertain if fingerprint cards are being held by NCIS Headquarters Records Department.
 - If subject received confinement, query brig records for the fingerprint card.
 - Determine whether or not FBI will accept military entry fingerprint cards for offenders.
 - If the above efforts fail to locate a suitable fingerprint card, submit the report directly to the National Instant Criminal Background Check System for entry. Estimated date of completion: TBD
- Submit disposition records for historical cases with fingerprints in NCIC but missing R84 submission. Estimated date of completion: TBD
- Recommend the approval of the comments from NCIS and OGC contained on the DD-818 provided at TAB A.

RECOMMENDATION: That SECNAV signs TAB A.

Approve_____ Disapprove_____

COORDINATION: TAB C

Attachments:

As stated

Prepared by: [REDACTED], NCIS, Criminal Investigations Directorate, [REDACTED].

Secretary of the Navy CNIC



DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET, SE, SUITE 1000
WASHINGTON NAVY YARD DC 20374-5140

5740
Ser N00/17U654
30 Nov 17

From: Commander, Navy Installations Command
To: Deputy Undersecretary of the Navy (Policy)

Subj: DEPARTMENT OF DEFENSE INSPECTOR GENERAL EVALUATION OF
FINGERPRINT CARD AND FINAL DISPOSITION REPORT SUBMISSION BY
MILITARY SERVICE LAW ENFORCEMENT ORGANIZATIONS. PROJECT NO.
2017-C002

Ref: (a) Draft Report - Evaluation of Fingerprint Card and Final Disposition Report
Submissions by Military Service Law Enforcement Organization (Project No. 2017-
C002)

1. The draft report evaluated whether DOD Law Enforcement Organizations (LEOs) submitted fingerprint cards and final disposition reports for military Service Members convicted by court-martial of qualifying offenses to the FBI Criminal Justice Information Services (CJIS) Division for inclusion in the FBI's Next Generation Identification database as required by DoD instruction.

2. Commander, Navy Installations Command (CNIC) concurs with the Recommendations in D.1 related to Finding D as they pertain to Navy Security Forces responsible for law enforcement activities that occur on Navy installations.

3. The following information is provided for Navy Security Forces assigned to CNIC in response to Recommendation D.1 related to Finding D.

a. Recommendation D.1.a.

(1) CNIC will direct Navy Security Forces under its cognizance to promptly take action to submit fingerprint cards and final disposition reports that are not in the FBI CJIS database.

(2) Estimated completion date is 31 January 2018.

b. Recommendation D.1.b.

(1) On 20 November 2017, CNIC initiated and directed all Navy Security Forces under its cognizance to conduct a comprehensive review of all entries in the Navy Criminal Law Enforcement Operations Center (CLEOC) database for qualifying offenses and verify compliance of fingerprint card and final disposition report submission in the FBI CJIS database.

(2) Estimated completion date of the review the CLEOC database is 8 December 2017.

c. Recommendation D.1.c.

Secretary of the Navy

CNIC (cont'd)

Subj: DEPARTMENT OF DEFENSE INSPECTOR GENERAL EVALUATION OF FINGERPRINT CARD AND FINAL DISPOSITION REPORT SUBMISSION BY MILITARY SERVICE LAW ENFORCEMENT ORGANIZATIONS. PROJECT NO. 2017-C002

(1) CNIC will ensure that command, supervisory, and management oversight controls over Navy Security Forces under its cognizance verify compliance with fingerprint card and final disposition report submissions as required by DoD instruction. CNIC will incorporate compliance verification as a special interest item in future IG inspections and conduct checks as part of the inspection cycle.

(2) Estimated completion date 30 September 2018.

d. Recommendation D.I.d.

(1) On 9 November 2017, CNIC initiated a comprehensive review of its criminal history reporting program including policy, training, fingerprint equipment, fingerprinting and final disposition report submission processes. CNIC will ensure the program is consistent with DoDI 5505.1 and implemented.

(2) Estimated completion date of the comprehensive review of its criminal history reporting program is 30 December 2017. Estimated completion date of corrective actions resulting from the review is 30 June 2018.

e. Recommendation D.I.e.

(1) CNIC will direct Naval Security Forces under its cognizance to conduct a review of all entries in the FBI CJIS database to ensure completeness.

(2) Estimated completion date is 30 June 2018.

f. Recommendation D.I.f.

(1) CNIC will revise NTTP 3-07.2.3 to align fingerprint and final disposition report submission to the FBI CJIS database requirements set forth in DoDI 5505.11.

(2) Estimated completion date is 31 January 2018.

4. My point of contact is [REDACTED], who may be reached at [REDACTED] or e-mail: [REDACTED].



M. M. JACKSON

Copy to:
CNO WASHINGTON DC (N4)
NAVIG WASHINGTON DC
OJAG WASHINGTON DC
CNIC WASHINGTON DC (N00, N3, IG)

Secretary of the Navy USMC



DEPARTMENT OF THE NAVY
HEADQUARTERS, UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5580
DMCS-A
1 Dec 17

FIRST ENDORSEMENT on DC, PP&O ltr 5580 Ser PPO of 30 Nov 17

From: Head, Audit Coordination, Office of the Director,
Marine Corps Staff
To: Office of the Secretary of the Navy

Subj: SERVICE RESPONSE TO SECNAV REGARDING DOD IG REPORT ON
EVALUATION OF FINGERPRINT CARD AND FINAL DISPOSITION
REPORT SUBMISSIONS BY MILITARY SERVICE LAW ENFORCEMENT
ORGANIZATIONS (PROJECT NO. 2017-C002)

Encl: (1) DC, PP&O correspondence 5580 over PPO dtd 30 Nov 17

1. Enclosure (1) is forwarded for Department of the Navy consideration in responding to DODIG Draft Evaluation Report Project No. 2017-C002.
2. We appreciate the opportunity to comment on the report.
3. For questions regarding this response, you may contact me at 703-697-1950/571-289-7082/or charles.dove@usmc.mil.

A handwritten signature in black ink, appearing to read "Charles K. Dove", is positioned above the printed name.

CHARLES K. DOVE

Copy to:
NAVINGEN (N14)
IGMC
CL
DC, P&R (MCMICP)
DC, PP&O

Secretary of the Navy
USMC (cont'd)



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

IN REPLY REFER TO:
5580
PPO
30 Nov 17

From: Deputy Commandant, Plans, Policies, and Operations
To: Secretary of the Navy
Via: Director, Marine Corps Staff

Subj: SERVICE RESPONSE TO SECNAV REGARDING DOD IG REPORT ON
EVALUATION OF FINGERPRINT CARD AND FINAL DISPOSITION REPORT
SUBMISSIONS BY MILITARY SERVICE LAW ENFORCEMENT
ORGANIZATIONS (PROJECT NO. 2017-C002)

Ref: (a) 2017-SECNAVGENCORRESPOND-000001155.002.002.001
Principal - STOPLIGHT - URGENT - SNGC (D) - EVALUATION OF
FINGERPRINT CARD AND FINAL DISPOSITION REPORT SUBMISSIONS
BY MILITARY SERVICE LAW ENFORCEMENT ORGANIZATIONS
(b) DoD IG Report Evaluation of Fingerprint Card and Final
Disposition Report Submissions by Military Service Law
Enforcement Organizations (Project No. 2017-C002)

Encl: (1) Response to U.S. Marine Corps Fingerprint and
Compliance (DODIG Recommendation G.1)

1. Per Ref (a), the Marine Corps provides the enclosed response to the subject draft report's findings and recommendations contained in Ref (b).
2. The Marine Corps concurs with the findings and recommendations, and is establishing a timeline to take corrective action.
3. The point of contact for this matter is [REDACTED], Head Law Enforcement, Investigations, and Corrections Branch at [REDACTED], [REDACTED]@usmc.mil.

A handwritten signature in black ink, appearing to read "B. D. Beaudreault".
B. D. BEAUDREULT

Secretary of the Navy USMC (cont'd)

U.S. Marine Corps Fingerprint and Disposition Compliance (DODIG Recommendation G.1)

Recommendation G.1.a. Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 37 fingerprint cards and 46 final disposition reports of the Marine Corps that are not on file in the Federal Bureau of Investigation Next Generation Identification database.

USMC Response: PSL, in coordination with MCI Command, has tasked all installation Provost Marshal's Offices (PMO) and Criminal Investigation Division (CID) offices to review all incident reporting and determine if the fingerprints of the suspect of the incident were taken, and submitted to the FBI, and if the disposition (command adjudication) was received from the command and submitted to the FBI. Additionally, PSL requested all locations to obtain a disposition for all suspects from the command or SJA, wherever possible, and those results would be provided to the FBI. The period covered is 01Jan15 through 31Oct17. The incidents referred to in this recommendation will be covered during this review. A suspense date of 08Dec17 was afforded to the PMO/CID's to accomplish the task.

Recommendation G.1.b. Immediately perform a comprehensive review of all Marine Corps criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.

USMC Response: Hard files of criminal investigative reports are only maintained on site for two years plus the current year to date. A current review is being conduct of all Military Police (MP) Incident Reports and CID Reports of Investigation (ROI) to determine compliance with DODI 5505.11. The period covered is 01Jan15 through 31Oct17.

The electronic database utilized by USMC Law Enforcement Consolidated Law Enforcement Operations Center (CLEOC) and only maintains MP Reports and CID ROI's that were initiated on or after 01Jan04. Hard files of fingerprint cards will not be available prior to 01Jan15; therefore, obtaining any fingerprint cards will be unlikely.

Conducting research back to the recommended date will take additional time and would require manpower and increased work hours to accomplish the task.

Recommendation G.1.c. Ensure Marine Corps command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure such compliance is included as a special interest item in IG inspections and is conducted.

Encl (1)

Secretary of the Navy USMC (cont'd)

U.S. Marine Corps Fingerprint and Disposition Compliance (DODIG Recommendation G.1)

USMC Response: The USMC IG functional area checklist for MP and CID addresses fingerprinting of suspects and collection of DNA; however, it is limited and will be updated.

Policy will be updated to spell out what the oversight controls will be.

Recommendation G.1.d. Conduct a comprehensive review of Marine Corps criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.

USMC Response: Law Enforcement Branch (PSL), Security Division, PP&O, HQMC, has recently participated in a rewrite of the USMC Law Enforcement Training and Readiness (T&R) Manual. The T&R manual for both MP's and CID Agents reflect a training task for taking suspect fingerprints IAW DODI 5505.11.

MCO 5580.2B w/CH 2, Chapter 16. Section 16303, Paragraph 4, defines procedures for USMC Law Enforcement personnel to take required suspect fingerprints and is consistent with DODI 5505.11.

MCO 5580.2B w/CH2 is currently under review for rewrite and will encompass policy, training, and process standards.

A training Course Content Review Board (CCRB) will be conducted for both the MP Basic Course and the CP Basic Officer Course to update their POIs to train to these standards.

Recommendation G.1.e. Also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

USMC Response: Collection of suspect DNA is also covered within MCO 5580.2B w/CH2.

The USMC IG checklist for both MP and CID will be updated to ensure that DNA is collected, processed, and submitted IAW the references.

Encl (1)

Secretary of the Air Force

AFOSI



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS
QUANTICO VIRGINIA



November 29, 2017

MEMORANDUM FOR DOD/IG

FROM: AFOSI/CC
27130 Telegraph Rd
Quantico, VA 27130

SUBJECT: Reference the DoD IG Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations (Project 2017-C002).

1. AFOSI concurs with the recommendations in Finding E, and offers these comments to each.
2. Recommendation E.1.a: Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 12 AFOSI fingerprint cards and 13 AFOSI final disposition reports that are not in the Federal Bureau of Investigation Next Generation Identification database.

Concur. Comment: Prior to receiving this report for comments, AFOSI had already taken steps to obtain fingerprint cards for the 12 subjects and index them into the National Crime Information Center (NCIC) and correct one subject without the proper disposition in NCIC. AFOSI searched digital databases, hardcopy case files, and contacted confinement facilities in an effort to remedy the missing indices.

- a. To date, AFOSI indexed three subjects and submitted a final disposition for one subject.
 - b. AFOSI is unable to index four subjects into NCIC due to missing or poor quality prints. However, three subjects were submitted to the National Instant Criminal Background Check System (NICS) for indexing. The other subject did not qualify since the drug conviction falls outside the time parameters (one year since conviction) for indexing in NICS.
 - c. AFOSI is awaiting responses from field units for fingerprints for three subjects.
 - d. No AFOSI criminal investigation file existed on two subjects identified by DoD IG. Both subjects returned negative results from a Defense Central Index of Investigations (DCII) check.
3. Recommendation E.1.b: Immediately perform a comprehensive review of all AFOSI criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.

"EYES OF THE EAGLE"

Secretary of the Air Force

AFOSI (cont'd)

Concur. Comment: Review was directed by order of the Secretary of the Air Force before receipt of this report.

4. Recommendation E.1.c: Ensure that AFOSI command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is included as a special interest item in AFOSI IG inspections, and is actually conducted.

Concur. Comment:

- a. Prior to receiving this report for comments, AFOSI instituted a three-tier process for reviewing NCIC indexing compliance at the field leadership, regional leadership, and headquarters level. This process requires attaching an NCIC Criminal History Report (CHR) reflecting indices for the investigation prior to case closure along with leadership notes indicating the CHR accurately reflects the results of the investigation. Headquarters level reviews are conducted prior to case file acceptance in the file room.
- b. In October 2017, the AFOSI Inspector General (IG) began inspecting AFOSI criminal indexing data as a special interest item during region unit effectiveness inspections. IG will work with functional managers to establish a permanent inspection checklist related to this area.

5. Recommendation E.1.d: Conduct a comprehensive review of AFOSI criminal history reporting programs to ensure all applicable agency policy, training, fingerprinting, and final disposition report submission processes are consistent with DoDI 5505.11, and are being implemented.

Concur. Comment:

- a. Prior to receiving this report for comments, AFOSI reviewed agency policy, training, fingerprinting, and final disposition report submission processes and determined they are in compliance with DoDI 5505.11, as it pertains to active duty suspects.
- b. AFOSI did identify the need for clarification to policy in DoDI 5505.11 pertaining to processing civilian suspects. AFOSI will coordinate with the DoD IG, in its capacity as the office of primary responsibility for DoDI 5505.11, for policy clarification.

6. Recommendation E.1.e: Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, have been submitted for inclusion in FBI databases.

Concur. Comment: Prior to receiving this report for comments, AFOSI initiated action to assess compliance with DNA sample submissions in accordance with DoDI 5505.14.

Secretary of the Air Force
AFOSI (cont'd)

7. I am available to provide additional details or answer any questions. You may contact me at kirk.stabler@us.af.mil or 571-305-8000.


KIRK B. STABLER, Colonel, USAF
Commander

Secretary of the Air Force

Air Force Security Forces



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC



22 November 2017

MEMORANDUM FOR DoDIG

FROM: HQ USAF/A4S
1030 Air Force Pentagon, Rm 5E1040
Washington, DC 20330-1030

SUBJECT: Air Force Security Forces Response to DoDIG Draft Report Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations, Project No. 2017-C002, dated 20 November 2017

1. Thank you for the opportunity to review and provide comment on the aforementioned draft report. Please note, overall, we concur with the recommendations and subsequently outline in paragraph two associated corrective actions. That said, given the importance of the report and the sensitivity of the subject, we are compelled to submit a three comments to the report itself:

Issue (Page 27): Current text reads as: “The Security Forces and Security Forces Investigators assigned to the Air Force Security Forces Center (AFSFC) typically investigate misdemeanor crimes in the Air Force, such as petty theft, simple assault, and traffic crimes.”

A4S Comment: This statement is factually inaccurate. Security Forces investigators are not assigned to the Air Force Security Forces Center. Investigators work for the squadron to which they are assigned. We can work with your office for corrective language but in no case do squadron investigators work for, or are they assigned to the Air Force Security Forces Center.

Issue (Page 29): In June 2017, Air Force Security Forces told us that units use the Management Internal Control Toolset (MICT), which is the Air Force’s centralized repository for inspection checklist and reporting. The Security Forces MICT checklist items are supposed to be monitored and assessed as part of the installation commander’s self-inspection program. Air Force Security Forces is required to conduct self-inspections of its programs and field units using the Security Forces MICT. The AFI 31-118 Security Forces MICT checklist has a line item to validate whether the fingerprinting procedures are being followed for criminal offenses in accordance with DoDI 5505.11. However, the checklist does not include fingerprint card and final disposition report submission compliance.

A4S Comment: If the fingerprinting procedures are followed IAW DoDI 5505.11, then per se procedures are being followed for fingerprint card and final disposition report submission. These activities are not mutually exclusive. If a unit is not following fingerprint card or final disposition report procedures, they should not be assessed as compliant with the MICT line item of the communicator.

BREAKING BARRIERS...SINCE 1947

Secretary of the Air Force

Air Force Security Forces (cont'd)

B. Issue (Page 29): We asked the AFSFC representative why Air Force Security Forces fingerprint card and final disposition report submission rates were deficient given the emphasis on training, and the units' oversight compliance checks.

A4S Comment: Manual fingerprint collection is inherently inefficient due to the number of rejections associated with inking procedures and the Security Forces inability to correct discrepancies on the spot. Crucial to our overall reduction in fingerprint submission errors and commensurate improvement in submission of final disposition reports is fully implementing digital fingerprint collection across the Security Force enterprise.

2. In addition to the above comments, please see the road ahead for the associated report recommendations:

Recommendation F.1.a.: Submit to the Federal Bureau of Investigation Criminal Justice Information Service the 93 Air Force Security Forces fingerprint cards and 93 Air Force Security Forces final disposition reports that are not on file in the Federal Bureau of Investigation Next Generation Identification database.

A4S Response: Concur. AFSFC reviewed the 93 records and 41 of 93 are loaded into NCIC Criminal history. We are working with responsible units to collect the remaining 52 for submittal.

Recommendation F.1.b.: Immediately perform a comprehensive review of all Air Force Security Forces criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.

A4S Response: Concur. We have initiated an audit of all of our accessible Security Forces case files and will work with the Federal Bureau of Investigation as necessary to resolve discrepancies as possible within the limits of the law.

Recommendation F.1.c.: Ensure Air Force Security Forces command, supervisory, and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure such compliance is included as a special interest item in future IG inspections, and is actually conducted.

A4S Response: Concur. The Air Force Director of Security Forces issued direction on 13 November 2017 for all Security Forces Squadrons to re-accomplish their applicable MICT communicator and to ensure compliance with law and policy. The Air Force Deputy Chief of Staff, Logistics, Engineering, and Force Protection reiterated this direction to the Major Commands on 19 November. We would welcome the Air Force Inspector General's inclusion of this item as a Special Interest Item in the future.

Recommendation F.1.d.: Conduct a comprehensive review of Air Force Security Forces criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.

Secretary of the Air Force

Air Force Security Forces (cont'd)

A4S Response: Concur. We have initiated a policy, process, and training review to ensure we are consistent with DoDI 5505.11 and to improve execution of these policies and procedures at the unit level.

Recommendation F.1.e.: Also, ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

A4S Response: Concur. We have incorporated these areas into our on-going policy, process, and training review.

Recommendation F.1.f.: Direct the Director of Air Force Security Forces to revise AFI 31-120 to align with final disposition report submission requirements set forth in DoDI 5505.11.

A4S Response: Concur. AF/A4S identified this discrepancy during the adjudication of comments associated with the October 2017 revision of AFI 31-120. This instruction is in final coordination and we anticipate official publication in 90 days.

3. Thank you for your time and consideration. My point of contact for this issue is [REDACTED], AF/A4SP at DSN [REDACTED].

TULLOS.ANDRE [REDACTED]
A.D. [REDACTED]
ANDREA D. TULLOS, Brig Gen, USAF
Director of Security Forces
DCS/ Logistics, Engineering, and Force Protection

Under Secretary of Defense for Intelligence



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

DEC 01 2017

MEMORANDUM FOR PRINCIPAL DEPUTY INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to Recommendations Contained in Evaluation of Fingerprint Card and
Final Disposition Report Submissions by Military Service Law Enforcement
Organizations

1. On 20 November 2017, the Department of Defense Office of the Inspector General (DoD IG) provided the Office of the Undersecretary of Defense for Intelligence (OUSDI) with a copy of the above-captioned report which contained specific recommendations for OUSDI related to the activities of the Defense Intelligence Agency (DIA), National Geospatial Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA). Specifically, DoD IG recommended that OUSDI work with these Defense Intelligence Components (DIC) to:

- a. Immediately perform a comprehensive review of all their criminal investigative databases and files to ensure all fingerprint cards and final disposition reports for anyone investigated for, or convicted of, qualifying offenses at least to 1998 have been reported to the FBI CJIS in compliance with DoD and FBI requirements.
- b. Ensure that supervisory and management oversight controls verify compliance with fingerprint card and final disposition report submission requirements and ensure that such compliance is regularly inspected.
- c. Conduct a comprehensive review of their criminal history reporting programs to ensure all fingerprinting and final disposition report submission policy, training, and processes are consistent with DoDI 5505.11, and have been implemented.
- d. Also ensure that other required investigative and criminal history information, such as criminal incident data and Deoxyribonucleic Acid (DNA) samples, has been submitted for inclusion in FBI databases.

2. OUSDI has reviewed these recommendations and agrees with DoD IG as to the advisability of performing these reviews. OUSDI will therefore engage with the noted DICs to validate their collection and reporting of fingerprint records and final disposition reports, and ensure that appropriate policies and controls exist in this regard and are consistent with DoDI 5505.11. Findings of this review, and any noted corrective actions, will be provided to DoD IG upon completion.

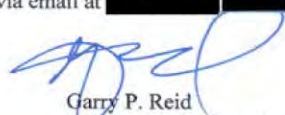
3. OUSDI also notes that DoD components beyond the DICs also maintain personnel and offices which conduct police-like functions similar to those of the DICs. As OUSDI does not



Under Secretary of Defense for Intelligence (cont'd)

maintain oversight of such entities, we recommend that DoD IG engage with these additional components to ensure that they are also in compliance with DoDI 5505.11, and other appropriate policies and procedures.

4. If further assistance or information is required, please contact the OUSD(I) POC, [REDACTED], at [REDACTED], or via email at [REDACTED]@mail.mil.



Garry P. Reid
Director for Defense Intelligence
(Intelligence & Security)

Deputy Chief Management Officer



DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

November 29, 2017

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: DoD IG Draft Report - "Evaluation of Fingerprint Card and Final Disposition Report Submission Requirements by Military Service Law Enforcement Organizations," Project Number 2017-C002

This is in response to your request for comments regarding the proposed subject report. I concur with the recommendations to the DoD Components outlined in the report as Recommendation H.1.

The Pentagon Force Protection Agency (PFPA) will conduct a comprehensive review to ensure all fingerprint cards and final disposition reports have been reported in compliance with the Department of Defense and Federal Bureau of Investigation requirements. PFPA will review their policy, training, processes, and oversight controls to ensure compliance with DoD Instruction (DoDI) 5505.11, Fingerprint Card and Final Disposition Report Submission Requirements. PFPA will complete this review and take corrective actions by 1 March 2018.

PFPA will ensure that other required investigative and criminal information is submitted for inclusion in the Federal Bureau of Investigation databases. PFPA is working with the Defense Management Data Center to develop a process to report information as required by DoDI 7730.47, Defense Incident-Based Reporting System (DIBRS). PFPA expects to have a solution by 1 March 2018. In accordance with DoDI 5505.14, Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, Law Enforcement, Corrections, and Commanders, PFPA is finalizing guidance to ensure the proper collection of DNA samples from suspects of criminal investigations. PFPA will publish guidance and implement collection of DNA samples by 1 February 2018.

If you have any questions, the point of contact for the Deputy Chief Management Officer is Mr. Jonathan H. Cofer, Director, PFPA. He can be reached at 703-693-3685 or jonathan.h.cofer.civ@mail.mil.

A handwritten signature in black ink, which appears to read "John H. Gibson II".

John H. Gibson II

Defense Criminal Investigation Service



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

December 04, 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR POLICY AND OVERSIGHT

SUBJECT: DoD IG Draft Report – “Evaluation of Fingerprint Card and Final Disposition Report Submissions by Military Service Law Enforcement Organizations” (Project No. 2017-C002)

In response to your request for comments on the referenced report, the Defense Criminal Investigative Service (DCIS), the criminal investigative component of the DoD OIG, agrees with your recommendations and provides the below comments outlining actions it is taking to ensure it has submitted required investigative and criminal history data for inclusion in FBI databases.

Specifically, DCIS initiated a comprehensive examination of all closed investigations, which will ultimately go back to 1998, to determine if it complied with reporting requirements. DCIS also directed a policy review to ensure its compliance with requirements conveyed in DoD Instruction 5505.11, “Fingerprint Card and Final Disposition Report Submission Requirements.” Additionally, DCIS will update case closure checklists to require mandatory validation of information submitted to the FBI. DCIS will also include validation of this information as a special interest item on future inspections of DCIS operations and will institute periodic spot checks of closed cases to evaluate the agency’s validation requirements.

We appreciate the opportunity to respond to your draft report. My point of contact for this response is Principal Deputy Director Kelly Mayo. He can be reached at Kelly.mayo@dodig.mil.

A handwritten signature in black ink, appearing to read "Dermot F. O'Reilly", is positioned above the typed name.

Dermot F. O'Reilly
Deputy Inspector General for Investigations

Acronyms and Abbreviations

ACMIS	Army Courts-Martial Information System
AFI	Air Force Instruction
AFOSI	Air Force Office of Special Investigations
AFSFC	Air Force Security Forces Center
AFTR	Air Force Training Record
AGCIC	Advanced General Crimes Investigation Course (AFOSI)
ALCID	All CID Elements Message
ALERTS	Army Law Enforcement Reporting and Tracking System
AMJAMS	Automated Military Justice Administration and Management System (Air Force)
AR	Army Regulation
BSIC	Basic Special Investigations Course (AFOSI)
CID	Criminal Investigation Division
CIDSAC	CID Special Agent Course (Army and Marine Corps)
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CJIS	Criminal Justice Information Services
CLEOC	Navy Consolidated Law Enforcement Operations Center
CMS	Case Management System (Navy and Marine Corps JAG)
CNIC	Commander, Navy Installations Command
DCIO	Defense Criminal Investigative Organizations
DCIS	Defense Criminal Investigative Service
DCMO	Deputy Chief Management Officer
D-Dex	Law Enforcement Defense Data Exchange
DoDI	Department of Defense Instruction
DoDIG	Department of Defense Inspector General
FBI	Federal Bureau of Investigation
FD	Federal Document
I2MS	Investigative Information Management System
IAFIS	Integrated Automated Fingerprint Identification System
IGI	Inspections Branch (AFOSI)
IMCOM	Installation Management Command (Army)
JABS	Joint Automated Booking Station (Air Force Security Forces)
JAG	Judge Advocate General
LEO	Law Enforcement Organization
MCIO	Military Criminal Investigative Organizations
MICT	Management Internal Control Toolset (Air Force)
MP	Military Police

Acronyms and Abbreviations (cont'd)

MPI	Military Police Investigations
MPR	Military Police Report (Army)
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NCOIC	Non-Commissioned Officer in Charge
NGI	Next Generation Identification
NJIS	Navy Justice Information System
NTTP	Navy Tactics, Techniques, and Procedures
OIC	Officer In Charge
OJT	On the Job Training
OPNAV	Chief of Naval Operations
ORI	Originating Agency Identifier
PMI	Program Management Inspections (Air Force Security Forces)
POST	Peace Officer Standards and Training
PQS	Personnel Qualification Standards (Navy)
R&A	Records and Analysis (Air Force Security Forces)
RIC	Regional Investigations Coordinator (NCIS)
SFMIS	Security Forces Management Information System (Air Force)
SJA	Staff Judge Advocate
SMART	Strategic Management Analysis and Reporting Tool – OSI (AFOSI)
SMARTNet	Security Management Automation Resource Tracking Network
SO	Security Officer (Navy Security Forces)
TCN	Transaction Control Number
TECOM	Training and Education Command (Marine Corps)
TRM	Training and Readiness Manual (Marine Corps)
U.S.C.	United States Code
UCR	Uniform Crime Reporting (FBI)
USACRC	U.S. Army Crime Record Center
USAFSIA	U.S. Air Force Special Investigations Academy
USAMPS	U.S. Army Military Police School
USD(I)	Under Secretary of Defense for Intelligence
USMC	United States Marine Corps



Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

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
Defense Hotline 1.800.424.9098

