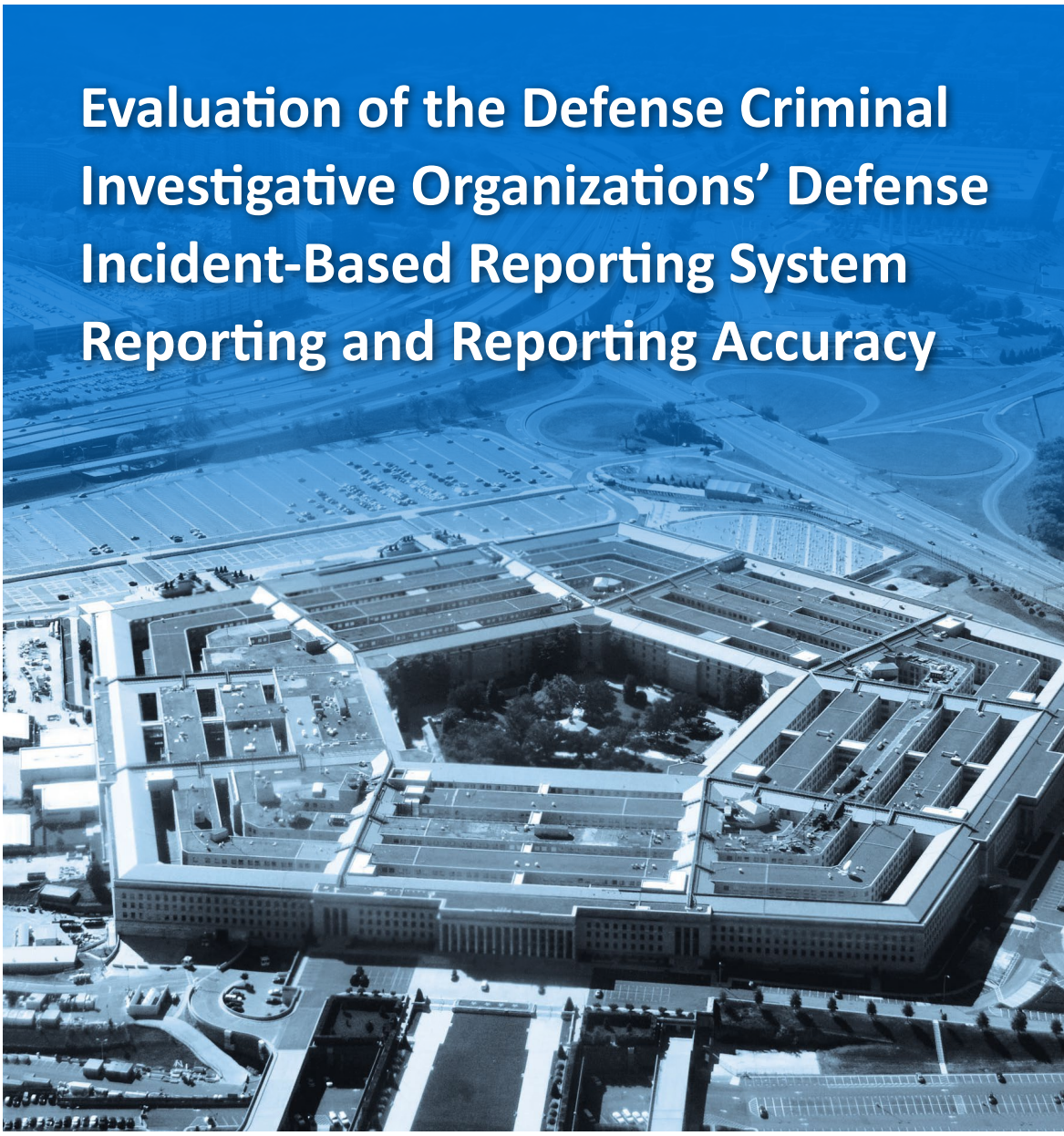
Report No. DODIG-2015-011

INSPECTOR GENERAL

U.S. Department of Defense

OCTOBER 29, 2014

Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
29 OCT 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,4800 Mark Center Drive,Alexandria,VA,22350-1500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**40**	

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.

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

Results in Brief

Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy

October 29, 2014

Objective

We 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.[1]

Finding

DoD is not reporting criminal incident data to the Federal Bureau of Investigation (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. The FBI uses the data to develop a reliable set of criminal statistics for U.S. law enforcement agencies.

Recommendations

- The Director, Defense Human Resources Activity, (DHRA), provide functional guidance to Defense Manpower Data Center (DMDC) and the DIBRS data submitters by reestablishing the cross-functional DIBRS Council to provide a forum for the exchange of information, best practices, and the continuing operation of the DIBRS, as required by DoDM 7730.47-M, Volume 1.

Recommendations (Cont'd)

- The Director, DHRA, obtain FBI certification for DIBRS, as required by DoDM 7730.47-M, Volume 1.
- The Director, DHRA, ensure DIBRS criminal incident data are reviewed and submitted to the FBI National Incident-Based Reporting System for inclusion in the annual Uniform Crime Reports, as required by DoDM 7730.47-M, Volume 1.
- The Director, DHRA, ensure DIBRS error corrections are tracked to completion as required by DoDM 7730.47-M, Volume 1.
- The Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations; Director, Defense Criminal Investigative Service ensure the DIBRS data submitters provide accurate and complete data submissions within 15 workdays after the end of each month as required by DoDM 7730.47-M, Volume 1.
- The Commander, U.S. Army Criminal Investigative Command; Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations ensure DIBRS error corrections are completed within 30 days of DMDC providing notification as required by DoDM 7730.47-M, Volume 1.

[1] We limited our review to the three Military Criminal Investigative Organizations (MCIOs) with accounts in DIBRS and Defense Criminal Investigative Service (DCIS), which currently does not have an account. We did not evaluate the remaining five DoD Components with accounts in DIBRS. DoDD 7730.47 tasks the DoD OIG with monitoring compliance with this instruction as it relates to the DCIOs.

Visit us at www.dodig.mil

Results in Brief

Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy

Management Comments

Overall, the Director, Defense Human Resources Activity concurred with our recommendation to obtain FBI certification for DIBRS, as required by DoDM 7730.47-M, Volume 1. The Commander, U.S. Army Criminal Investigative Command; Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations and the Director, Defense Criminal Investigative Service concurred with their respective recommendations concerning providing accurate and complete data, and completing DIBRS error corrections.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
The Director, DHRA		1.a, b, c and d
Commander, U.S. Army Criminal Investigative Command		2.b
Director, Naval Criminal Investigative Service		2.a and b
Commander, Air Force Office of Special Investigations		2.a and b
Director, Defense Criminal Investigative Service		2.a

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

October 29, 2014

MEMORANDUM FOR DIRECTOR, DEFENSE HUMAN RESOURCES AGENCY
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy (Report No. DODIG-2015-011)

This final report is provided for information and use. We evaluated the Defense Criminal Investigative Organizations' (DCIOs) process for reporting accurate criminal incident data to the Defense Incident-Based Reporting System (DIBRS) in accordance with DoD Directive 7730.47 and DoD Manual 7730.47 M, Volume 1, "Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements," December 7, 2010. "Defense Incident-Based Reporting System (DIBRS).

We found DoD does not report criminal incident data to the Federal Bureau of Investigation (FBI) as required by the Uniform Federal Crime Reporting Act of 1988 and DoD Directive 7730.47.

We considered management comments on a draft of this report when preparing the final report. The Director, Defense Human Resources Activity concurred with our recommendation to obtain FBI certification for DIBRS, as required by DoDM 7730.47 M, Volume 1. The Commander, U.S. Army Criminal Investigative Command; Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations and the Director, Defense Criminal Investigative Service concurred with their respective recommendations concerning providing accurate and complete data, and completing DIBRS error corrections.

Management's comments were responsive to the draft and conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the review staff. For additional information on this report, please contact Mr. Jeff Bennett, Director of Oversight, (703) 699-5667.

Randolph R. Stone
Deputy Inspector General
Policy and Oversight

Contents


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

We evaluated the Defense Criminal Investigative Organizations' (DCIOs) process for reporting accurate criminal incident data to the Defense Incident-Based Reporting System (DIBRS) in accordance with DoD Directive 7730.47,[2] and DoD Manual 7730.47-M, Volume 1, "Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements," December 7, 2010. Specifically, we focused on:

- Whether the DCIOs followed established procedures for reporting incidents to the Defense Manpower Data Center (DMDC);
- How the DCIOs ensured incidents were correctly reported;
- How the DCIOs ensured that DIBRS reporting was accurate; and
- Whether DIBRS criminal incident data reporting complied with Federal law and DoD policy and guidance.

Background

The DoD Office of Inspector General (OIG) initiated this project to evaluate whether the DCIOs' DIBRS criminal incident data reporting complied with Federal law and DoD policy and guidance as set forth in DoD Directive 7730.47 and DoD Manual 7730.47-M, Volume I.

The Uniform Federal Crime Reporting Act of 1988 (28 U.S.C 534 note), as amended requires the United States Attorney General to collect and preserve national data on Federal criminal offenses as part of the Uniform Crime Reports (UCR) Program. The program was conceived in 1929 by the International Association of Chiefs of Police to meet the need for reliable uniform crime statistics. The Act directs Federal agencies that routinely investigate complaints of criminal activity to report details about such crimes to the Attorney General. The Federal Bureau of Investigation (FBI) was designated as the central collection point for criminal incident data reporting. The FBI's National Incident-Based Reporting System (NIBRS)

[2] The governing guidance during the period of our review was the standard outlined in DoD Directive 7730.47 (certified current as of December 1, 2003). After completing our DIBRS Program review but prior to publishing our report, OUSD (P&R) reissued DoD Directive (DoDD) 7730.47 as DoD Instruction (DoDI) 7730.47 (dated January 23, 2014). Not withstanding the issuance of DODI 7730.47, all references in this report are to DoDD 7730.47, which was in effect during the evaluation period, unless otherwise noted. We analyzed DoDI 7730.47 and found it does not affect the findings or recommendations we identified during our review.

(its crime reporting system) was designed to collect and store data on each crime occurrence and on each incident and arrest within that occurrence. The FBI uses the data to develop a reliable set of criminal statistics for law enforcement agencies throughout the country to use in their administration, operation, and management.

Additional data collection and reporting requirements are contained in the Victims' Rights and Restitution Act of 1990 (49 U.S.C. 10601 note) and the Brady Handgun Violence Prevention Act (18 U.S.C. 921 note).

The DCIOs conduct investigations meeting the mandatory data collection and reporting requirements of the Uniform Federal Crime Reporting Act of 1988, Victims' Rights and Restitution, and Brady Handgun Violence Prevention Acts. DoD Directive 7730.47, "Defense Incident-Based Reporting System (DIBRS)," December 1, 2003, and DoD Manual 7730.47-M implements those Federal laws. The Directive and the Manual require DoD Components with law enforcement, criminal investigative, military justice, and corrections functions to comply with the crime reporting requirements contained in the Acts.[3]

To comply with the requirements, DoD created the DIBRS, a central repository of incident-based statistical data maintained and operated at the DMDC, which reports to Office of the Under Secretary of Defense (Personnel and Readiness) (OUSD (P&R)). The DIBRS database maintained by the DMDC is the tool the DoD uses to collect and transmit NIBRS reportable criminal incident data for use in the FBI's Uniform Crime Report Program.

DoD Directive 7730.47 assigned the Under Secretary of Defense for Personnel and Readiness (USD[P&R]) responsibility for developing policy for DIBRS and to monitor compliance with the Directive (see footnote 3).

DoD Directive 7730.47 designated the Director of Law Enforcement Policy and Support (LEPS), Defense Human Resources Activity (DHRA), Office of the Under Secretary of Defense for Personnel and Readiness (OUSD (P&R)), the Principal Staff Assistant for purposes of overseeing DIBRS implementation.

[3] We limited our review to the three Military Criminal Investigative Organizations (MCIOs) with accounts in DIBRS and the Defense Criminal Investigative Service (DCIS), which currently does not have an account. We did not evaluate the remaining five DoD Components with accounts in DIBRS. The DoDD 7730.47 tasks the DoD OIG with monitoring compliance with this instruction as it relates to the DCIOs.

Finally, DoD Manual 7730.47-M, Volume 1, requires agencies to provide DIBRS with criminal incident data 15 days after the end of each month. DMDC is required to return submissions containing errors with full explanations and descriptions of the errors. The submitting agency makes corrections and resubmits the data within 30 days. Submission of errors is required to be tracked to completion by DMDC and the submitting agencies.

Finding

DoD Is Not Reporting Criminal Incident Data to the FBI for Inclusion in the Uniform Crime Reports As Required by Federal Law

As a result, 10 years of DoD criminal incident data have not been provided 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 UCR Program, as implemented in DoD Directive 7730.47 and DoD Manual 7730.47-M, Volume 1.

The Uniform Federal Crime Reporting Act of 1988 requires the United States Attorney General to collect and preserve national data on Federal criminal offenses as part of the UCR Program. The Act directs Federal agencies that routinely investigate complaints of criminal activity to report details about crimes to the Attorney General. DoD policies such as DoD Manual 7730.47-M, Volume 1, implements those Federal laws and requires DoD Components with law enforcement, criminal investigative, military justice, and corrections functions to comply with the crime reporting requirements.

DoD Directive 7730.47 required the OUSD (P&R) to ensure that DMDC formulates a data collection mechanism to track and report DIBRS information from initial contact through investigation, prosecution, confinement, and release and to report NIBRS data to the FBI.

DMDC formulated a data collection mechanism to track and report DIBRS information, but DMDC never completed the FBI's certification requirements to report NIBRS data to the FBI, which is contrary to DoD Directive 7730.47.

DoD Has Started but Not Completed the Requirements for DIBRS System Certification

For an agency to submit criminal incident data to NIBRS for inclusion in the annual uniform crime reports, the FBI's Criminal Justice Information System (CJIS) Division, Crime Statistics Management Unit, Uniformed Crime Reporting Office, must first certify the agency's data system.

The CJIS NIBRS Coordinator stated DoD must meet certain criteria in order to obtain system certification. The criteria are: (1) system appropriateness: the agency must provide evidence their NIBRS-reporting system is compatible with the FBI's UCR system; (2) update capability and responsiveness: the agency must demonstrate its ability to update submissions, meet deadlines, respond to FBI queries and requests, and correct errors received from the FBI UCR Program in a timely manner; and (3) error rate: requires a sustained error rate of 4 percent or less for three separate data submissions. Refer to Appendix B for additional information on the NIBRS certification requirements.

The CJIS NIBRS Coordinator stated DoD does not yet meet criterion (2) update capability and responsiveness. He added that a contributing agency must, at minimum, maintain a 2-year (retention period) database of NIBRS submissions and have the capability to update incidents from the previous calendar year. The CJIS NIBRS Coordinator told us it was his understanding DIBRS contributors submit incidents when the case is closed. He also reported it was his understanding if there are errors, DMDC lacks the ability to require the DoD contributors to modify or correct the data on a closed incident and DMDC is unsure how to resolve this issue.

The DMDC DIBRS Database Administrator confirmed the DoD DIBRS data system is not certified by the FBI. He stated in order to obtain FBI certification, DMDC had to provide 3 months of data with a less than 3 percent error rate. The DMDC DIBRS Database Administrator told us they were close to achieving the 3 percent error rate. According to CJIS, the acceptable error rate is less than 4 percent, and DoD is meeting the requirement. The DMDC DIBRS Database Administrator was also aware that DMDC had to demonstrate the ability to correct errors and resubmit corrected or error-free data. The DMDC DIBRS Database Administrator did not complete the NIBRS certification due to his belief the reporting agencies do not have the resources to retroactively correct data. The DMDC DIBRS Database Administrator stated in October 2012, the issue was brought to the attention of the Director of Law Enforcement Policy and Support, DHRA, OUSD (P&R), who has responsibility for oversight of DMDC and the DIBRS program. The Director of Law Enforcement Policy and Support, DHRA, OUSD (P&R), reported he was not aware if the DCIOs had sufficient personnel or what training each DCIO provided to personnel responsible for DIBRS reporting.

DoD Does Not Have a Process to Ensure DIBRS Submitting Agencies Provided DIBRS Data 15 Workdays After the End of Each Month

DoD Manual 7730.47-M, Volume 1, states:

> All DIBRS data submitters shall prepare reports using the specified reporting procedures and submit them 15 workdays after the end of each month.

The Director of Law Enforcement Policy and Support, DHRA, OUSD (P&R), is responsible for developing policy for DIBRS. The Director stated although there is a requirement for monthly reporting to DIBRS by the MCIOs, it is not an issue if they are a month behind in reporting. We learned DIBRS continuously updates database information, and data reported a month late gets updated in subsequent monthly submissions.

The DMDC DIBRS Database Administrator stated the submitting agencies report criminal incident information to DMDC on a monthly basis within the first 15 days of the month, as required by DoD Manual 7730.47, Volume 1. However, if the submitting agencies have problems with their information technology (IT), data errors, or if there is a change in personnel administering the DIBRS function, it may delay their reporting submissions. During our review we noted Air Force Office of Special Investigations (AFOSI) was not reporting DIBRS information during the period of August 2012 through January 2013. The DIBRS reporting lapse was due to the AFOSI DIBRS program administrators departing before replacements were trained on their responsibilities. The reporting lapse was immediately corrected based on our observation.

DIBRS Errors

Each MCIO has a separate account on DMDC's secure server to connect and transfer the data from their systems to DMDC. When DMDC receives the data, it is run through a series of testing programs that check each data element and compare it to the requirements. If the MCIO's data elements are incorrect, an error report is created on a particular record. Once the testing is complete, DMDC creates an error report, which identifies the number of records in error. DMDC forwards the error report to the MCIOs to correct the data and resubmit it. According to the DIBRS Database Administrator, DMDC's role is to analyze the data against published DIBRS values, provide feedback to submitting agencies

on data not adhering to policy, and archive and report the data to NIBRS. As the originators of the DIBRS information, the MCIOs are responsible for DIBRS data input and are thus responsible for correcting errors identified by DMDC.

Each DCIO Had a Different Process for Correcting DIBRS Errors

DCIS

While DCIS investigates various offenses that are DIBRS reportable, the DCIS Project Manager, Case Reporting Information Management System (CRIMS), stated DCIS has not reported DIBRS information to DMDC. The CRIMS Project Manager did suggest that some DCIS investigative data; i.e., criminal incident data, may still have been reported to DIBRS by DCIS investigative partners in joint investigations. DCIS originally anticipated DIBRS reporting would be incorporated into version 1 of its new CRIMS. However, DCIS reported that in order to meet its Initial Operating Capability, DCIS could fund only its primary mission requirements and could not meet unfunded mandates such as DIBRS reporting. DCIS leadership stated the DIBRS reporting requirement would be incorporated into CRIMS version 2.

Army

The Deputy Chief Information Officer, Office of the Army Chief Information Officer (G-6), U.S. Army Criminal Investigation Command (USACIDC) Headquarters (HQ), is responsible for reporting criminal incident data to DIBRS. HQ USACIDC reports the most current criminal incident data information through a secure file transfer protocol on or about the 4th day of each month, meeting the requirement to report by the 15th day of the month as mandated by DoD Manual 7730.47-M, Volume 1. The Deputy Chief Information Officer estimated that USACIDC's monthly error rate was 10 percent.

HQ USACIDC does not actually correct the erred data. Rather, the method HQ USACIDC used to resolve (correct) the errors was to "strip" (omit) the errors from the report. Instead of replacing the erred data with correct data, they enter "NULL" in the data field, thus eliminating any DIBRS database conflicts. They resubmit the still uncorrected data to DMDC, usually by the 15th of the month. He explained "stripping the errors" was a more efficient way to manage the timeliness of DIBRS submissions because CID does not have a process to obtain corrected data from the originating investigative field unit.

Navy

The Naval Criminal Investigative Service (NCIS) DIBRS Program Manager, Consolidated Law Enforcement Operations Center (CLEOC) Directorate, Headquarters, NCIS, stated NCIS submits criminal incident data to DMDC on the 15th of every month. The NCIS IT Specialist and CLEOC Database Administrator, who is responsible for submitting criminal incident data to DMDC, stated NCIS rarely receives error reports from DMDC, but when they do, DMDC forwards the error reports by e-mail. The NCIS DIBRS Program Manager explained they have a pre-check process that checks data prior to submission to DMDC to ensure there are no errors. NCIS uses the DMDC-provided edit checker to check for errors in the data prior to submitting the data to DMDC. If the edit checker finds no errors in the data, the data is sent to DMDC. If there are errors, the edit checker checks the data again in subsequent monthly submissions.

For example, in its February 2013 submission, NCIS had a total of 2,097 incidents that qualified for DIBRS submission. According to the NCIS IT Program Manager for CLEOC, the 2,097 incidents included new and updated criminal incident data entered in its system combined with incorrect or erred data from previous months. Of the 2,097 incidents, 121 were error-free and submitted to DIBRS. The remaining 1,976 incidents contained errors of some type and were not submitted to DMDC.

The NCIS DIBRS Program Manager explained that the 1,976 cases containing errors would not be corrected. NCIS' DIBRS submissions consist of closed cases and NCIS has no process in place for correcting errors in closed cases. Furthermore, the 1,976 cases will be resubmitted monthly and will fail again. The NCIS DIBRS Program Manager explained NCIS does not have the time, money, or resources to correct the errors.

Air Force

The HQ Air Force Office of Special Investigation IT Enterprise Management Directorate (HQ AFOSI/XIW), Investigative Information Management System (I2MS) Program Manager, explained AFOSI submits criminal incident data to DMDC on a monthly basis, however, he did not know the exact date AFOSI makes submission to DMDC. DMDC returns data identified as incorrect or in error to AFOSI. HQ AFOSI forwards the incorrect information to the original submitting AFOSI detachment to correct the data submission. The AFOSI detachment corrects the data and resubmits to HQ AFOSI. He stated he was not aware of a timeline to correct the information and return it to DMDC, but the units usually correct data errors within 2 days. He was

not aware of any suspense for having the errors completed and returned to DMDC. The I2MS Program Manager further stated the DIBRS error rate HQ AFOSI received from DMDC was approximately 1 to 3 percent. The HQ AFOSI assessment division randomly reviews 15 to 20 percent of the cases to ensure correct DIBRS reporting.

DMDC and the DCIOs Do Not Ensure Corrections to DIBRS Submission Errors Are Tracked to Completion

DoD Manual 7730.47-M, Volume 1, as applied to the submitting agencies, states:

> DMDC shall return submissions containing errors with appropriate error notification to the submitting agency. The submitting agency shall make the appropriate corrections and resubmit the report within 30 days. Data submitted to DMDC is edited in accordance with the requirements specified in both volumes of this Manual. In addition, if data element 5, REPORTABLE TO NIBRS, is "Y," additional edit checks are performed in accordance with the FBI requirements specified in Volumes 1 to 4 of Reference (n). All errors shall be returned to the submitting agency with full explanations and descriptions. All data submission errors shall be tracked to completion, and;
>
> [DIBRS submitting agencies shall] coordinate file-naming conventions and security of data with DMDC before the initial transmission of data via the Defense Information Systems Network or a comparable data network. Submitting organizations are responsible for the accuracy and completeness of each electronic data transfer.

The DoD Director of Law Enforcement Policy and Support explained there was no negative impact if the errors were not corrected within 30 days because the incident data contained in the DIBRS database is continually being updated by the submitting agencies. Finally, he stated that he thought the DMDC DIBRS Database Administrator was responsible for tracking errors and ensuring they are forwarded to the appropriate agency and corrected.

The DMDC Database Administrator maintains copies of the error reports he sends, but does not track the errors to ensure corrections are made. He does not track or review data, he only loads data and updates the DIBRS system. He stated data that passes DIBRS validation is considered correct; but it is the Services' responsibility to ensure the data is accurate and correct. He explained he does not have the authority to give the submitting agencies a suspense for correcting and returning the data.

Conclusion

Our evaluation determined DoD has not completed the FBI's requirements for the DIBRS database certification; therefore, DoD does 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.

Although 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 is aware of the FBI's requirements to obtain certification, but has 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.

Our evaluation determined DoD's ability to submit criminal incident data to the NIBRS database as mandated by DoD Directive 7730.47 could be impacted due to the submitting agency's (MCIO's) inaccurate and/or incomplete DIBRS criminal incident data reporting to the DMDC. DoD, through DMDC, does not have a process to ensure the DCIOs submit required criminal incident data by the 15th of each month. Additionally, DoD, through DMDC, does not have a process to ensure identified criminal incident data errors are tracked to correction. Furthermore, we discovered one DCIO is not reporting DIBRS data; one DCIO is reporting a small percentage of criminal incident data collected; and one DCIO is not correcting data. Only one DCIO appeared to submit corrections to criminal incident data.

Recommendations, Management Comments and Our Response

Overall, the Defense Human Resources Activity (DHRA) and the Defense Criminal Investigative Organizations (DCIOs) agreed with our report and recommendations. We received management comments on a draft of this report. The comments addressed our assessment of DIBRS reporting status. The management comments are summarized and addressed below, and included verbatim as Management Comments.

Recommendation 1

1a. The Director, Defense Human Resources Activity, (DHRA), provide functional guidance to Defense Manpower Data Center (DMDC) and the DIBRS data submitters by reestablishing the cross-functional DIBRS Council to provide a forum for the exchange of information, best practices, and the continuing operation of the DIBRS, as required by DoDM 7730.47-M, Volume 1.

DHRA Comments

DHRA partially concurred with recommendation 1a and provided: The DIBRS Council has effectively never dissolved; it has morphed into and been absorbed by a broader governance of DoD law enforcement agency criminal justice information (CJI) collection, sharing, and reporting post nine eleven (sic). While DIRBS reporting is still important, DoD has put its limited resources toward developing a new CJI reporting system. The CJI system is piloting a new process to extract UCR (DIBRS) data from law enforcement agency databases thereby removing the need for the DIBRS database. However, to the extent that priorities permit and resources are available, the Department will continue to provide a forum for the exchange of information, best practices, and the continuing operation of the DIBRS.

Our Response

The management comments are responsive to our recommendation. Our evaluation noted continuing questions and issues from the DCIOs revolving around DIBRS data submission. Since the new CJI system is still in the data testing phase and does not yet have the ability to extract UCR (DIBRS) data, the DIBRS Council has a continuing need to meet and discuss DIBRS issues.

1b. The Director, DHRA, obtain FBI certification for DIBRS, as required by DoDM 7730.47-M, Volume 1.

1c. The Director, DHRA, ensure DIBRS criminal incident data are reviewed and submitted to the FBI National Incident-Based Reporting System for inclusion in the annual Uniform Crime Reports, as required by DoDM 7730.47-M, Volume 1.

1d. The Director, DHRA, ensure DIBRS error corrections are tracked to completion as required by DoDM 7730.47-M, Volume 1.

DHRA Comments

DHRA concurred with recommendations 1b, 1c, and 1d, and provided: DoD's final certification requirement involves a timely return of corrected data. DMDC's goal has been to obtain the error report from the FBI and correct the error checking software so that these errors will be caught during the period when the data is submitted to DIBRS. This will allow DMDC to address the bad data at the front end of the process instead of the back end (with FBI checks). The DIBRS Database Administrator is working with his FBI CJIS counterpart to work out a plan for the error correction testing process.

Our Response

The management comments are responsive to our recommendations. DHRA's plan to work with their FBI CJIS counterpart, as outlined in their response, should help DoD gain system certification and accomplish data submission and tracking requirements.

Recommendation 2

2a. The Commander, U.S. Army Criminal Investigative Command; Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations; Director, Defense Criminal Investigative Service ensure the DIBRS data submitters provide accurate and complete data submissions within 15 workdays after the end of each month as required by DoDM 7730.47-M, Volume 1.

Army Comments

The US Army Criminal Investigation Command's (USACIDC) non-concurred with recommendation 2a and provided: USACIDC does submit DIBRS data, as required, within the 15 day window of each month.

Our Response

The USACIDC management comment is responsive to our recommendation. We validated USACIDC submits their DIBRS data within 15 workdays after the end of each month. Therefore, we have removed the USACIDC from recommendation 2a.

Navy Comments

The US Naval Criminal Investigative Service (NCIS) concurred with recommendation 2a and provided: NCIS will continue to submit DIBRS data on the 15th of each month via the Consolidated Law Enforcement Operations Center (CLEOC), which is the criminal case management system for the Department. To reduce the number of errors encountered, NCIS (as the program manager for CLEOC) is reemphasizing to all users the need to provide accurate and complete information when entering DIBRS required data into CLEOC.

Our Response

The NCIS management comments are responsive are responsive to recommendation 2a.

Air Force Comments

The United States Air Force Office of Special Investigations (AFOSI) concurred with the recommendation 2a and provided: AFOSI identified and corrected the internal process flaw which allowed a lapse in reporting to occur, and as of 10 July 2014, the DIBRS program managers completed corrective action. The OSI Investigative Information Management System (12MS) program managers now track the monthly data submissions to ensure OSI DIBRS data will be accurate and complete.

Our Response

The AFOSI management comments are responsive to recommendation 2a.

DCIS Comments

The Defense Criminal Investigative Service (DCIS) concurred with the factual statements in the draft report that DCIS is not reporting DIBRS data and provided: DCIS anticipates DIBRS reporting will be addressed subsequent to the deployment of CRIMS v.2 which is on hold while information technology funding and budget issues are being addressed OIG-wide. If and when DCIS is able to deploy CRIMS v.2, they anticipate DIBRS compliance within six months of deployment, depending on required funding and contract support.

DCIS added there is a supportable and rational basis for their lack of compliance with DIBRS reporting requirements. DCIS provided DIBRS does not actually report the information it collects to the FBI's National Incident-Based Reporting System (NIBRS) as intended; DIBRS has not received certification for reporting to NIBRS; DIBRS is expected to be replaced by the CJI sharing system (D-DEx); and CRIMS v.2 is expected to be CJI sharing system compliant for the purposes of DIBRS criminal investigative data reporting.

Our Response

The DCIS management comments are responsive to recommendation 2a. While we note DCIS' rationale for their non-compliance with DIBRS reporting requirements, The Uniform Federal Crime Reporting Act of 1988 (28 U.S.C 534 note) requires Federal agencies to report UCR data. DoD Directive 7730.47, "Defense Incident-Based Reporting System (DIBRS)," December 1, 2003, and DoD 7730.47-M implements the Federal law. The Directive and the Manual require DoD Components with law enforcement, criminal investigative, military justice, and corrections functions to comply with the crime reporting requirements.

2b. The Commander, U.S. Army Criminal Investigative Command; Director, Naval Criminal Investigative Service; Commander, Air Force Office of Special Investigations ensure DIBRS error corrections are completed within 30 days of DMDC providing notification as required by DoDM 7730.47-M, Volume 1.

Army Comments

The US Army Criminal Investigation Command (USACIDC) concurred with recommendation 2b and provided: The USACIDC does not currently have a method nor the resources (personnel and/or systems funding) to correct all rejected/error files that are returned from DIBRS. The USACIDC will be fielding a new information system, Army Law Enforcement Reporting and Tracking System, in January 2015, which should reduce the number of errors.

Our Response

The USACIDC management comments are responsive to recommendation 2b. The USACIDC official reported their organization does not have the resources to reduce the amount errors. Although, USACIDC is hopeful their new reporting system will result in the reduction of DIBRS errors.

Navy Comments

The US Naval Criminal Investigative Service (NCIS) concurred with recommendation 2b and provided: NCIS is developing mechanisms and procedures to ensure errors are corrected in CLEOC within 30 days of notification by DMDC. Additionally, processes to ensure accuracy and completeness of DIBRS data will be built into the new Department of the Navy Naval Justice Information System (NJIS), currently under development and scheduled for implementation in FY2015.

Our Response

The NCIS management comments are responsive to recommendation 2b. The NCIS reporting official explained they developed the CLEOC reporting system with new mechanisms to correct errors. They are hopeful the NJIS reporting system will ensure better accuracy and completeness of DIBRS data.

Air Force Comments

The AFOSI concurred with recommendation 2b and provided: AFOSI identified and corrected the internal process flaw which allowed this lapse to occur, and as of 10 July 2014, the DIBRS program managers completed corrective action. The OSI Investigative Information Management System (12MS) program managers now track the monthly data submissions to ensure OSI DIBRS data will be accurate and complete.

Our Response

The AFOSI management comments are responsive to recommendation 2b. The AFOSI official reported the managers of the DIBRS data submission have identified and corrected internal flaws. Also, the new AFOSI reporting system will track monthly data submissions for accuracy and completeness.

Appendix A

Scope and Methodology

We conducted this assessment from February 2013 to October 2013 in accordance with the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Inspections and Evaluations," January 2012. Based on the assessment objectives, we planned and performed the evaluation to obtain sufficient information to provide a reasonable basis for our observations and conclusions, based on our assessment objectives.

Our work included a review of each submitting agency's policies and procedures for collecting and reporting data regarding criminal incidents. We reviewed the processes used by submitting agencies to meet mandatory reporting requirements for criminal activities and examined the reporting mechanisms/systems used for automated reporting. We examined the types of data the submitting agencies report to DIBRS.

Additionally, we evaluated how the submitting agencies processed DIBRS data errors for correction and resubmission to DMDC. We interviewed the DoD Director of Law Enforcement Policy and Support, the DMDC DIBRS System Administrator, and key DCIO staff and analyzed criminal investigative database reports for a specified time period.

We identified relevant Federal statutes and DoD Directives and other guidance. We reviewed the Services' and Agency's policies and procedures guiding criminal incident reporting mechanisms. We conducted a data call for each submitting agency's criminal incident reporting requirements and instructional material pertaining to automated reporting systems. We determined how each agency complies with federally mandated DIBRS reporting standards as supplemented by DoD, Service, and submitting agency policy guidance.

As a result of the review and analysis of data call information, we interviewed the DoD Director of Law Enforcement Policy and Support, the DMDC DIBRS Database Administrator, and key DCIO staff to verify the results of the analysis and to obtain additional information.

Finally, we determined the process the submitting agencies use to ensure accurate reporting of criminal activities to DIBRS. We reviewed policy guidance and documents to validate the submitting agencies processes concerning accurate reporting.

Use of Computer-Processed Data

We used computer-processed data obtained from the DIBRS database. The DIBRS database administrator provided spreadsheets consisting of DIBRS error reports that were used in our analysis. Error reports were used as a tool to review the types and numbers of errors the DIBRS database administrator returned to the various submitting agencies for correction. Although there was no way of validating whether the submitting agencies corrected the information, the error reports provided a valuable insight into the complexity of the reporting requirements.

Prior Coverage

No prior coverage has been conducted on DIBRS reporting and reporting accuracy during the last 5 years.

Appendix B

NIBRS Certification Requirements

For an agency to submit criminal incident data to NIBRS, the FBI's Criminal Justice Information System (CJIS), Crime Statistics Management Unit, Uniformed Crime Reporting Office, must certify the agency's data system. The FBI uses the following criteria to grant a UCR Program or Law Enforcement Agency (LEA) NIBRS certification:

1. System Appropriateness: A UCR Program or Law Enforcement Agency must provide evidence their NIBRS-reporting system is compatible with the FBI's UCR system and follows NIBRS technical specifications. A UCR Program or LEA seeking NIBRS certification must submit its incident-based system's description including submission structure, crime categories, segment relationships, number of offenses collected per incident, and data values allowed per data element. The FBI will review this document for program design and concept.

2. Update Capability and Responsiveness: A UCR Program or LEA must demonstrate its ability to update submissions, meet deadlines, respond to FBI queries and requests, and correct errors received from the FBI UCR Program in a timely manner. A UCR Program or LEA must, at a minimum, maintain a 2-year database of NIBRS submissions (retention period) and have the capability to update incidents from the previous calendar year.

3. Error Rate: Data submissions must be logical and consistent. The FBI measures logic by the percent of Group A Incident Report submissions containing an error. The FBI defines the error rate as the number of rejected reports over the number of reports submitted. The FBI requires a sustained error rate of 4 percent or less for three separate data submissions. The applicable errors are included in the NIBRS Technical Specification.

4. Statistical Reasonableness: Data submissions must be statistically reasonable as a whole (in comparison to national trends). Although the error rate assesses the existence of logical mechanical flaws in the data, it does not address data in the aggregate. The FBI UCR Program evaluates aggregate data submissions in terms of percent distribution, data trend, volume, and monthly fluctuations.

Appendix C

References

The Uniform Federal Crime Reporting Act of 1988 (28 U.S.C. 534 note), the Victims' Rights and Restitution Act of 1990 (42 U.S.C. 10601 note), and the Brady Handgun Violence Prevention Act (18 U.S.C. 921 note) require all departments and agencies within the Federal Government (including the Department of Defense), which routinely investigate complaints of criminal activity, shall uniformly report details about crime within their respective jurisdiction to the United States Attorney General. The Attorney General shall acquire, collect, classify, and preserve national data on Federal criminal offenses as part of the UCRs.

DoD Directive 7730.47, now DoD Instruction 7730.47, and DoD Manual 7730.47-M, Volume 1, implement those Federal laws and require the DCIOs to establish procedures within their respective Military Services to report specific data elements to comply with those Federal reporting mandates. Additionally, the above DoD policies require the establishment and maintenance of a central database regarding incidents of domestic violence involving members of the Military Services. The central repository of criminal incident data is designed to enhance DoD's effectiveness in responding to Executive, legislative, and ad hoc requests for statistical information relating to criminal and other high-interest incidents. DIBRS is the DoD's centralized database system.

Annually, the DCIOs open investigations meeting the mandatory reporting requirements under the Uniform Federal Crime Reporting Act of 1988 (28 U.S.C. 534 note), the Victim's Rights and Restitution Act of 1990 (42 U.S.C. 10601 note), and the Brady Handgun Violence Prevention Act (18 U.S.C. 921 note).

The Uniform Federal Crime Reporting Act of 1988 requires the Attorney General to collect and preserve national data on Federal criminal offenses as part of the UCRs. The Act directs all Federal agencies that routinely investigate complaints of criminal activity to report details about such crimes to the Attorney General in a uniform manner and on a form prescribed by the Attorney General. The Act requires the Attorney General to distribute such details in the form of annual UCRs for the United States to the President, the Congress, State governments, and officials of localities and institutions participating in the UCR Program. The Act authorizes the Attorney

General to designate the FBI as the lead agency for performing the functions authorized by this Act and to establish such advisory boards as may be necessary to assist the Bureau. The Act requires the Director of the Bureau to classify offenses involving illegal drugs and drug trafficking as a part I crime in the UCRs. Finally, the Act authorizes appropriations.

Since the inception of the UCR Program in 1930, the FBI has been collecting crime data on offenses and arrests from approximately 16,000 county, state, and Federal law enforcement agencies. The FBI uses the data to develop a reliable set of criminal statistics for law enforcement agencies throughout the country to use in their administration, operation, and management.

During the late 1970s, the law enforcement community expanded the use of the UCR Program and developed new guidelines for reporting crime statistics. These guidelines formed the basis of NIBRS, as mandated by The Uniform Federal Crime Reporting Act of 1988, as amended. NIBRS requires law enforcement agencies, including those within the Department of Defense, to report NIBRS data to the Department of Justice for inclusion in the FBI-maintained system pursuant to FBI handbook.

The FBI assembles, publishes, and distributes the data to contributing agencies, including the Department of Defense, State UCR programs, Government bodies, and others interested in the Nation's crime problem. Law enforcement agencies consider NIBRS data to be an indispensable tool in the war against crime because it provides them with detailed, accurate, and meaningful statistical data about when and where crime takes place, what form it takes, and the characteristics of its victims and perpetrators. Law enforcement personnel and Government agencies armed with this information can request and allocate resources, and inform interested parties on the effort to combat crime.

The Victims' Rights and Restitution Act of 1990 requires all Federal law enforcement agency officers and employees to make their best efforts to accord victims of crime with the right to: (1) be treated with fairness and respect for the victim's dignity and privacy; (2) be protected from their accused offenders; (3) be notified of court proceedings; (4) attend public court proceedings related to the offense under certain conditions; (5) confer with the Government attorney assigned to the case; (6) restitution; and (7) information about the conviction, sentencing, imprisonment, and release of the offender.

As stated in DoD Manual 7730.47-M, Volume 1: Pursuant to The Victims' Rights and Restitution Act of 1990, as amended, victims and selected witnesses must be notified of their rights at certain phases of the case, from the time of initial contact by law enforcement through the investigation phase, prosecution phase, and, if the case results in confinement, the change in confinement status. The confinement authority must advise the victim or witness of an inmate's status, to include length of sentence, anticipated earliest release date, place of confinement, the possibility of transfer, the possibility of parole or clemency, release from confinement, escape, and death. DoD Instruction 1030.2, "Victim and Witness Assistance Procedures," requires the use of DD Form 2705, "Victim/Witness Notification of Inmate Status," for this purpose. The DIBRS requires that the number of victim and witness notifications be reported to DMDC in accordance with The Victims' Rights and Restitution Act of 1990, as amended.

The Brady Handgun Violence Prevention Act states that a licensed dealer shall not transfer a firearm to any other person who is not licensed without completing a background check or three business days elapsing. The Act directed the Attorney General to establish a national instant criminal background check system within 5 years of enactment. The Act requires the purchaser of a firearm to provide a statement that he or she is not under indictment or convicted of a crime, a fugitive from justice, addicted or unlawful user of a controlled substance, "mentally defective" or been committed to a mental institution, dishonorably discharged from the Armed Services, an undocumented individual, or renounced American citizenship to the local chief law enforcement officer.

According to DoD Manual 7730.47-M, Volume 1, the DIBRS shall be used to centralize the collection of information that is reportable by the DoD Components pursuant to The Brady Handgun Violence Prevention Act, which requires the Department of Defense to report these categories listed in the previous paragraph, to the FBI for purposes of prohibiting firearm purchases by certain select individuals.

Management Comments

DHRA Comments

DEFENSE HUMAN RESOURCES ACTIVITY
HEADQUARTERS
4800 MARK CENTER DRIVE, SUITE 06J25-01
ALEXANDRIA, VA 22350-4000

JUL 25 2014

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to DoD IG Draft Report, "Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy" (Project No. C2013-C003)

In response to the June 23, 2014, request for comments on an update to the Department of Defense Inspector General (DoD IG) Report C2013-C003, we provide the following comments pertaining to the DoD IG recommendations for the Director, Defense Human Resources Activity (DHRA).

Recommendation 1. We recommend the Director, DHRA:

a. Provide functional guidance to the Defense Manpower Data Center (DMDC) and the Defense Incident-Based Reporting System (DIBRS) data submitters by reestablishing the cross-functional DIBRS Council to provide a forum for the exchange of information, best practices, and the continuing operation of the DIBRS, as required by Department of Defense (DoD) Manual (DoDM) 7730.47-M, Volume 1.

DHRA Response: Partially Concur. When the DIBRS Council, in support of the newly created DIBRS, was established in the late 1990s, it was a standalone governance body for a standalone single purpose Criminal Justice Information (CJI) collection and reporting system. The DIBRS Council has effectively never dissolved; it has morphed into and been absorbed by a broader governance of DoD law enforcement agency CJI collection, sharing, and reporting post nine eleven.

While the DIBRS purpose of Uniformed Crime Reporting (UCR) is still important, it has taken a back seat to the need for CJI sharing among law enforcement agencies for crime, terrorism, and insider threat prevention and criminal investigative closure. DoD has put its limited resources into staying abreast of this need to share CJI, both within the Department and with civilian law enforcement surrounding DoD installations. The culmination of this effort is DoD's Law Enforcement Defense Data Exchange (D-DEx). This system enables DoD's law enforcement agencies to share CJI with each other, and with the majority of law enforcement agencies in the country, through various regional CJI sharing systems and the Federal Bureau of Investigation's (FBI) Law Enforcement National Data Exchange (N-DEx).

The FBI's Criminal Justice Information Services (CJIS) Division has recognized this reprioritization and is piloting a new process to extract UCR data from law enforcement agency live information sharing feeds to N-DEx. This will allow law enforcement agencies to keep the priority of effort on CJI sharing, at the national level, and simultaneously have their UCR data extracted for the National Incident-Based Reporting System (for UCR purposes). This will ultimately alleviate the need for maintaining old single purpose UCR systems such as DIBRS.

DHRA Comments (cont'd)

DoD is now in the data test phase between D-DEx and N-DEx, with the intention of going into production as soon as possible. Once D-DEx is in production with N-DEx and the FBI's UCR extraction process is established, DoD will look to begin submitting its UCR data in that manner.

To the extent that priorities permit and resources are available, the Department will continue to provide a forum for the exchange of information, best practices, and the continuing operation of the DIBRS. Ultimately, when D-DEX is providing both CJI for Law Enforcement sharing and UCR purposes, DIBRS will be terminated as a reporting system and archived.

b. Obtain FBI certification for DIBRS, as required by DoDM 7730.47-M, Volume 1.

DHRA Response: Concur. DoD's final certification requirement involves timely return of corrected data. DMDC's goal has been to obtain the error report from the FBI and correct the error checking software so that these errors will be caught during the period when the data is submitted to DIBRS. This will allow DMDC to address the bad data at the front end of the process instead of the back end (with FBI checks). The DIBRS Database Administrator is working with his FBI CJIS counterpart to work out a plan for the error correction testing process.

c. Ensure DIBRS criminal incident data are reviewed and submitted to the FBI National Incident-Based Reporting System for inclusion in the annual Uniform Crime Reports, as required by DoDM 7730.47-M, Volume 1.

DHRA Response: Concur. See 1.b. above.

d. Ensure DIBRS error corrections are tracked to completion as required by DoDM 7730.47-M, Volume 1.

DHRA Response: Concur. See 1.b. above.

I appreciate the opportunity to respond to your draft report. My point of contact for this response is [redacted]

Pamela S. Mitchell
Director

CIDC Comments

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

REPLY TO
ATTENTION OF

SEP 02 2014

CIIM-ZA

MEMORANDUM FOR U.S. Army Audit Agency (SSAG-PMO-L), 3101 Park Center Drive, Alexandria, VA 22303-1596

SUBJECT: Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System (DIBRS) Reporting and Reporting Accuracy

1. In response to Project No. C2013-C003, the U.S. Army Criminal Investigation Command (USACIDC) submits the following:

a. Recommendation 2a: Ensure DIBRS data is submitted within 15 days of each month.

Response: NON-CONCUR with recommendation table on page iii, listing ARMY USACIDC to respond to recommendation 2a since the DODIG stated on page 7 of the report that Army USACIDC met the requirement to report by the 15th day of the month. Delete 2a from the recommendation table and delete USACIDC from the first sentence of the Recommendation 2 listing all MCIOs to implement corrective action.

b. Recommendation 2b: Ensure errors are corrected within 30 days of notification by Defense Manpower Data Center, in accordance with Department of Defense (DoD) Manual 7730.47-M, Volume 1, 7 December 2010, subject: Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements.

Response: CONCUR with comment; Recommendation table on page iii, listing ARMY USACIDC to respond to recommendation 2b. USACIDC is fielding a new Army Law Enforcement Reporting and Tracking System (ALERTS) by January 2015 that should reduce the number of errors needing to be corrected. Errors will be reviewed for feasibility of correction and current practices will be continued to reduce database processing errors. However, the USACIDC does not currently have a method nor the resources (personnel and/or systems funding) to correct all rejected/error files that are returned from DIBRS.

2. The point of contact this action is [redacted]

FOR c/s
JOHN G. VOORHEES, JR.
COL, MP
Deputy Commander

Printed on Recycled Paper

NCIS Comments

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

August 15, 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL, POLICY AND OVERSIGHT, DEPARTMENT OF DEFENSE OFFICE OF INSPECTION GENERAL

SUBJECT: NCIS Response to the Report on the Evaluation of the Defense Criminal Investigative Organizations (DIBRS) Reporting (Project No. C2013-C003)

Ref: (a) DoDIG Report of 23 Jun 14

1. The Naval Criminal Investigative Service (NCIS) reviewed the reference, concurs with the findings and recommendations, and provides the following summary of actions to implement the recommendations.

a. Recommendation 2a: The Department of the Navy will continue to submit DIBRS data on the 15th of each month via the Consolidated Law Enforcement Operations Center (CLEOC), which is the criminal case management system for the Department. To reduce the number of errors encountered, NCIS (as the program manager for CLEOC) is reemphasizing to all users the need to provide accurate and complete information when entering DIBRS required data into CLEOC.

b. Recommendation 2b: NCIS is developing mechanisms and procedures to ensure errors are corrected in CLEOC within 30 days of notification by DMDC. Additionally, processes to ensure accuracy and completeness of DIBRS data will be built into the new Department of the Navy Naval Justice Information System (NJIS), currently under development and scheduled for implementation in FY2015.

2. The NCIS point of contact for the matter is [redacted] who can be reached at [redacted]

Samuel G. Worth
Principal Executive Assistant
Director

AFOSI Comments

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

24 July 2014

MEMORANDUM FOR DOD/IG

FROM: AFOSI/CC
27130 Telegraph Road
Quantico, VA 22134

SUBJECT: AFOSI Response to Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System (DIBRS) Reporting and Reporting Accuracy (Project No. C2013-C003) dated 23 June 2014

1. I concur with the finding and recommendations stated. We have identified and corrected the internal process flaw which allowed this lapse to occur, and as of 10 July 2014, my DIBRS program managers completed corrective action. The OSI Investigative Information Management System (I2MS) program managers now track the monthly data submissions to ensure OSI DIBRS data is accurate and complete.

2. My DIBRS/I2MS program managers are available if your staff has any questions. They are [redacted]

KEITH M. GIVENS
Brigadier General, USAF
Commander

"EYES OF THE EAGLE"

DCIS Comments

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

INFO MEMO

July 25, 2014

FOR: DEPUTY INSPECTOR GENERAL FOR POLICY AND OVERSIGHT

FROM: Ross Weiland, Assistant Inspector for Investigations – Internal Operations

WEILAND.ROSS.WILLIAM.1006134293 Digitally signed by WEILAND.ROSS.WILLIAM.1006134293 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODIG, cn=WEILAND.ROSS.WILLIAM.1006134293 Date: 2014.07.25 12:05:25 -04'00'

SUBJECT: Comments to IPO Draft Report on Evaluation of DCIO's DIBRS Reporting and Reporting Accuracy (Project No. C2013-C003)

- The purpose of this memorandum is to provide you with comments to the IPO Draft Report entitled Evaluation of the Defense Criminal Investigative Organizations' Defense Incident-Based Reporting System Reporting and Reporting Accuracy (Project No. C2013-C003).

- We have no issue with the factual statements in the draft report pertaining to DCIS. See p.7, Draft Report. I would note, however, that since we provided your staff with this information, circumstances surrounding the development and deployment of our CRIMS system have changed. We now anticipate that DIBRS reporting will be addressed subsequent to the deployment of CRIMS v.2. As of today, deployment of CRIMS v.2 is on hold while information technology funding and budget issues are being addressed OIG-wide. If and when we are able to deploy CRIMS v.2, we anticipate DIBRS compliance within 6 months of deployment, depending on required funding and contract support.

- Of greater concern is the absence in the Draft Report of the rationale behind DCIS's lack of DIBRS reporting compliance, or any mention of the DoD's Law Enforcement Defense Data Exchange (D-DEx).

- We note the following:
  - DIBRS does not actually report the information it collects to the FBI's National Incident-Based Reporting System (NIBRS) as intended;
  - DIBRS has not received certification for reporting to NIBRS;
  - DIBRS is expected to be replaced by D-DEx; and
  - CRIMS v.2 is expected to be D-DEx compliant.

- There is a supportable and rational basis for DCIS's lack of compliance with DIBRS reporting requirements and our preference would have been to include such rationale in the report.

Prepared by: Ross Weiland, AIG-I for Internal Operations, 703-604-8603

Acronyms and Abbreviations

ACI2	Automated Criminal Investigation Criminal Intelligence Information (CID)
AFOSI	Air Force Office of Special Investigations
CID	U.S. Army Criminal Investigations Command
CJIS	Criminal Justice Information Division
CLEOC	Consolidated Law Enforcement Operations Center (NCIS)
CRIMS	Case Reporting Information Management System (DCIS)
DCIO	Defense Criminal Investigative Organization
DCIS	Defense Criminal Investigative Service
DIBRS	Defense Incident-Based Reporting System
DHRA	Defense Human Resources Activity
DMDC	Defense Manpower Data Center
FBI	Federal Bureau Of Investigation
I2MS	Investigative Information Management System (AFOSI)
LEA	Law Enforcement Agency
LEPS	Law Enforcement Policy and Support
MCIO	Military Criminal Investigative Organization
NCIS	Naval Criminal Investigative Service
NIBRS	National Incident-Based Reporting System
OIG	Office of the Inspector General
OUSD (P&R)	Office of the Under Secretary of Defense for Personnel and Readiness
UCMJ	Uniform Code of Military Justice
UCR	Uniform Crime Report
USACID	U.S. Army Criminal Investigations Division
U.S.C	United States Code


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

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

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098