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

April 18, 2017
Ref: FOIA-2016-00797

SENT VIA EMAIL TO: john@greenewald.com
Mr. John Greenwald
The Black Vault
[redacted]

Dear Mr. Greenwald:

This is in response to your September 28, 2016, Freedom of Information Act (FOIA) request for a copy of report DODIG-2016-110, Evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures. We received your request on September 28, 2016, and assigned it case number FOIA-2016-00797.

The Office of the Deputy Inspector General for Intelligence and Special Program Assessments conducted a search and found the enclosed document responsive to your request. I determined that some redacted portions are exempt from release pursuant to 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy.

Additionally, the United States Army Intelligence and Security Command reviewed the report and determined that other portions are exempt from release in accordance with 5 U.S.C. § 552 (b)(1), which pertains to information that is currently and properly classified pursuant to Executive Order 13526, Section 1.4(c), intelligence activities (including covert actions), intelligence sources or methods, or cryptology; and 5 U.S.C. § 552 (b)(3), information exempted from release by statute, in this instance 50 U.S.C. § 3024(i), intelligence sources and methods.

In view of the above, you may consider this to be an adverse determination that may be appealed to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Your appeal, if any, must be postmarked within 90 days of the date of this letter and should reference the file number above. I recommend that your appeal and its envelope both bear the notation “Freedom of Information Act Appeal.”

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or https://ogis.archives.gov/. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one’s own records).

April 18, 2017
Ref: FOIA-2016-00797

If you have any questions regarding this matter, please contact the Department of Defense, Office of Inspector General FOIA Requester Service Center at 703-699-7498 or via email to foiarequests@dodig.mil.

Sincerely,

Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

~~SECRET//NOFORN~~

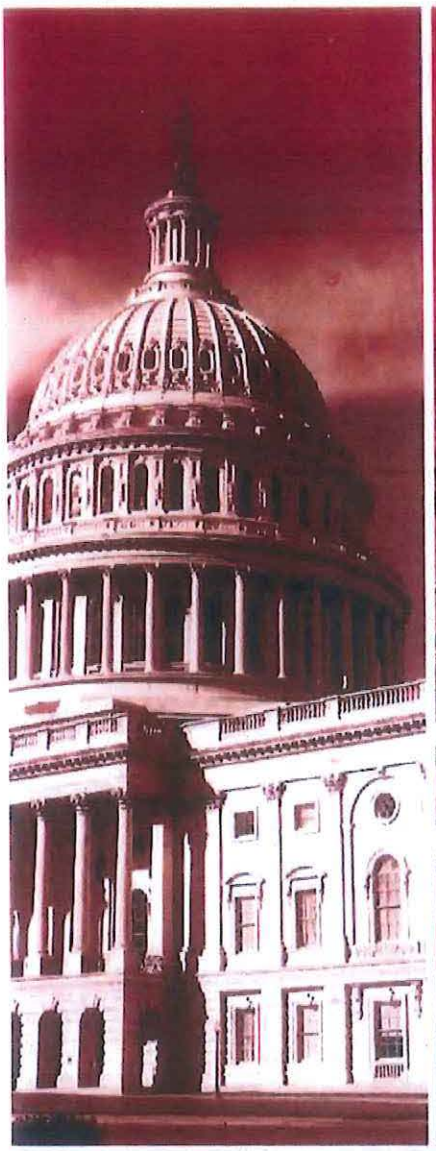
Report No. DODIG-2016-110

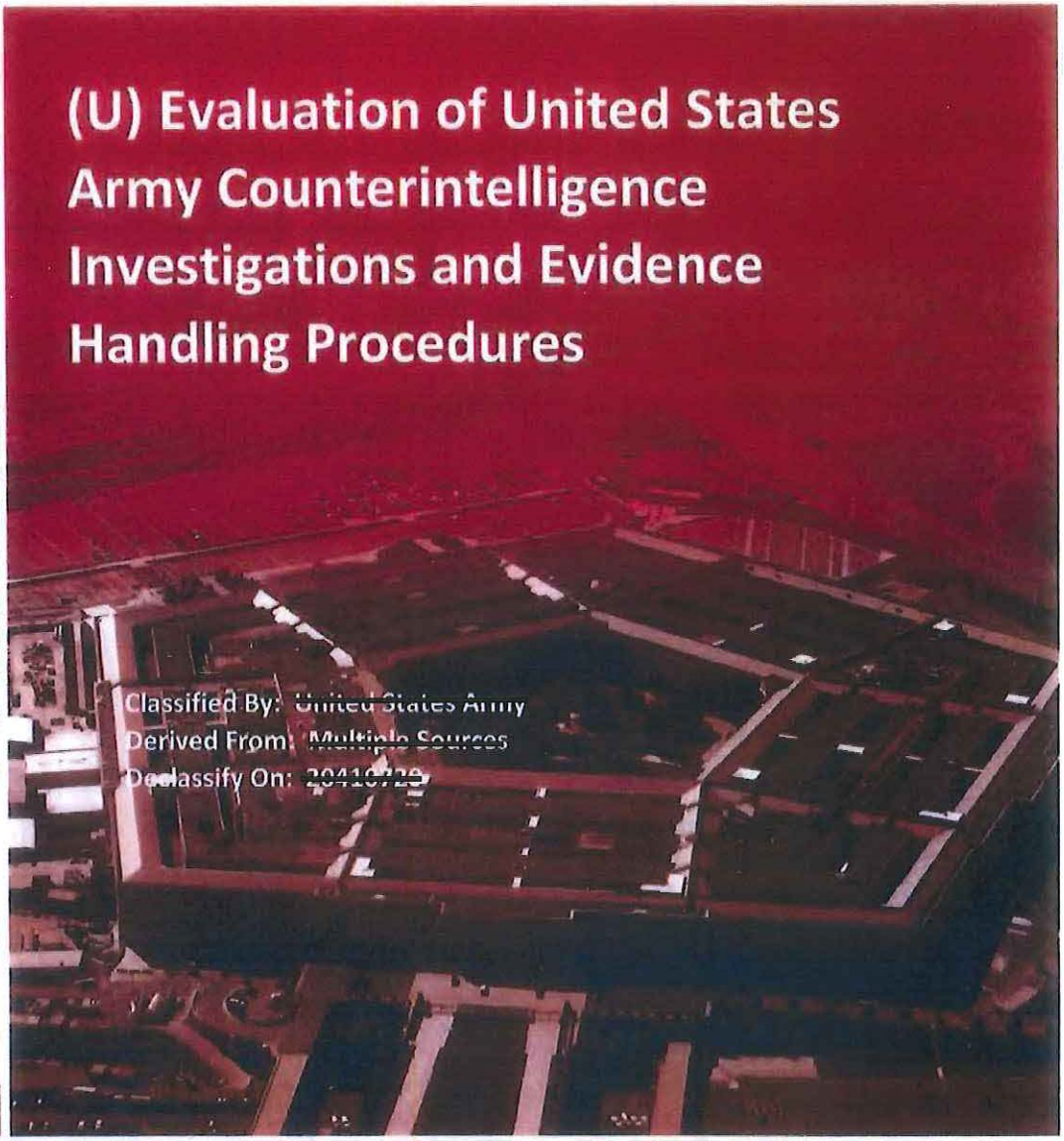
INSPECTOR GENERAL

U.S. Department of Defense

July 13, 2016

(U) Evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures





Classified By: ~~United States Army~~
Derived From: ~~Multiple Sources~~
Declassify On: ~~20410729~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

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.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Results in Brief

(U) Evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures

(U) July 13, 2016

(U) Objective

(U) Our objective was to determine whether continental United States Army counterintelligence investigative activities and evidence handling procedures complied with Executive Order 12333, DoD policy, and U.S. Army regulations.

(U) Findings

(U) Overall, we found that the Army is conducting counterintelligence investigative activities and evidence handling procedures in accordance with Executive Order 12333, DoD policy, and U.S. Army regulations. However, we found that the Army does not have a policy for entering subjects of Limited Counterintelligence Assessments into the Defense Central Index of Investigations as outlined by DoD Instruction 5505.07, "Titling and Indexing Subjects of Criminal Investigations in the Department of Defense," January 27, 2012; Army Regulation 381-10, "U.S. Army Intelligence Activities, May 3, 2007; and Army Regulation 381-45, "Investigative Records Repository," May 31, 2013. A Limited Counterintelligence Assessment is a local file initiated to determine if an incident or matter is of counterintelligence interest.

(U) Recommendations

(U) We recommend that the Director, U.S. Army Counterintelligence, Human Intelligence, Disclosure and Security (G-2X), authorize sending Limited Counterintelligence Assessments to the Investigative Records Repository so subject information from Limited Counterintelligence Assessments can be indexed into the Defense Central Index of Investigations as is done with Preliminary Investigations and Full Field Investigations.

(U) Management Comments and Our Response

(U) The Army G-2 concurred with and addressed the specifics of Recommendation B.1. We do not require any further management comments. Please see the Recommendations Table on the next page.

(U) Recommendations Table

(U) Management	Recommendations Requiring Comment	No Additional Comments Required
Director, U.S. Army Counterintelligence, Human Intelligence, Disclosure and Security (G-2X)	None	B.1

(U)

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

July 13, 2016

(U) MEMORANDUM FOR DEPARTMENT OF THE ARMY, OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2

SUBJECT: (U) Evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures (Report No. DODIG-2016-110)

(U) We are providing this final report for your information and use. This report relates to the U.S. Army's counterintelligence investigations and evidence handling procedures and was completed in accordance with the OIG's oversight responsibilities, as described in Section 8L of the Inspector General Act of 1978, as amended.

(U) Our evaluation was conducted to determine whether continental United States Army counterintelligence investigative activities and evidence handling procedures complied with Executive Order 12333, DoD policy, and U.S. Army regulations. Overall, the Army is conducting counterintelligence investigative activities in accordance with established policy.

(U) We considered management comments on the draft of this report. The United States Army G-2 concurred with Finding B and the recommendation. We do not require any further management comments.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7430 or DoD OIG: (b) (6) at DoD OIG: (b) (6)

Anthony C. Thomas
Deputy Inspector General for
Intelligence and Special
Program Assessments

This Page Left Blank Intentionally

(U) Contents

(U) Introduction

(U) Objective

(U) Our objective was to determine whether continental United States Army Counterintelligence (CI) investigative activities, and evidence handling procedures, complied with Executive Order 12333, DoD policy, and U.S. Army regulations.

(U) Applicable Criteria

(U) Executive Order 12333, "United States Intelligence Activities"

(U) DoD Directive 5240.01, "DoD Intelligence Activities," dated August 27, 2007 (Incorporating Change 1 and Certified Current Through August 27, 2014)

(U) DoD 5240.01-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," dated December 1982

(U) Army Regulation (AR) 381-10, "U.S. Army Intelligence Activities," dated May 3, 2007

(U) AR 381-12, "Threat Awareness and Reporting Program," dated October 4, 2010

(U) AR 381-20, "The Army Counterintelligence Program," dated May 25, 2010

(U) AR 381-45, "Investigative Records Repository," dated May 31, 2013

(U) AR 195-5, "Evidence Procedures," dated February 22, 2013.

(U) Executive Order 12333, as amended, identifies the intelligence and CI elements of the Army, Navy, Air Force, and Marine Corps as elements of the Intelligence Community. It directs the commanders and heads of those elements to collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and CI to support departmental requirements and, as appropriate, national requirements. The order also directs the Secretary of Defense to protect the security of DoD installations, activities, information, property, and employees by appropriate means, including investigation of applicants, employees, contractors, and other persons with similar associations with the DoD, as are necessary. The order specifies that

(U) elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned (or by the head of a department containing such element) and approved by the Attorney General of the United States consistent with the authorities provided by Part I of the order, after consultation with the Director of National Intelligence. Executive Order 12333 serves as the basis for the following DoD and Army intelligence and counterintelligence policy guides: DoD 5240.01, DoD 5240.01-R, AR 381-10 and AR 381-20.[1] DoD Directive 5240.01 is the primary authority used by Defense Intelligence Components that allows CI elements to collect, process and retain, or disseminate information concerning U.S. persons. DoD 5240.01-R implements DoD Directive 5240.01 and allows DoD intelligence components to carry out their authorized functions while ensuring that their activities which effect U.S. persons are carried out in a manner that protect the constitutional rights and privacy of U.S. persons. AR 381-10 includes guidance on the conduct of intelligence collection techniques by Army components and provides reporting procedures for certain Federal crimes. AR 381-12 details what incidents and behaviors are reportable to Army counterintelligence personnel. AR 381-20 specifies policy, standards, responsibilities, authorities, and procedures for all aspects of the

(U) Army Counterintelligence Programs to include CI investigative activities. AR 195-5 dictates the evidence handling procedures that are applicable to Army counterintelligence personnel.

(U) Background

(U) CI and espionage investigations are some of the most sensitive and complicated activities within the investigative realm. Specifically, CI and espionage investigations of U.S. citizens have heightened sensitivity and scrutiny due to protections under U.S. laws that citizens have regarding privacy. The U.S. Army Criminal Investigation Division is responsible for investigating all felonies with an Army nexus. U.S. Army counterintelligence special agents conduct investigations in the United States and

[1] AR 381-20, Chapter 4.

(U) worldwide to detect, identify, assess and counter, neutralize, or exploit the foreign intelligence, foreign adversary, international terrorist, and insider threat to the Army and DoD.[2]

(U) According to entrance briefings we received, the 308th Military Intelligence (MI) Battalion (BN) is responsible for conducting continental United States Army CI investigations. Personnel assigned to local field offices of the 308th MI BN conduct Army CI investigations. The field offices report to one of the four companies that make up the 308th MI BN. The 308th Special Investigations Detachment has a worldwide mission and conducts high visibility CI investigations. The 308th MI BN provides investigative support elements, and the 310th MI BN provides technical investigative support. The 902nd MI Group has command and control of the 308th and 310th MI BNs.

(U) Management and oversight of continental United States (CONUS) CI investigations is conducted through several leadership echelons and includes personnel from the 308th, the 902nd by means of the CONUS Counterintelligence Coordinating Authority (CICA), (and at the G-2X level through the US Army Counterintelligence Coordinating Authority (ACICA). Approval authorities for the majority of investigative processes are several layers above the operational level of CI investigations. (See Appendix B.)

(U) The Army has three categories of CI investigations: Limited Counterintelligence Assessments (LCA), Preliminary Investigations (PI), and Full Field (FF) Investigations. AR 381-20, "The Army Counterintelligence Program," defines LCAs, PIs, and FFs. The LCA may be conducted upon receipt of information that indicates a potential foreign intelligence or international terrorist threat to the Army or DoD. The LCA is initiated to facilitate the proactive collection of information regarding those threats. An LCA determines whether the incident or matter is of counterintelligence interest prior to opening a formal investigation. The PI is a limited duration inquiry into the circumstances surrounding a reported incident, or matter of potential counterintelligence interest, to determine if there are specific facts giving reason to believe that a threat to national security may exist. Finally, the FF investigation is

[2] Ibid

(U) conducted when there are specific and articulate facts giving reason to believe that individuals under Army CI jurisdiction are involved in acts that may constitute threats to national security. An LCA may normally be authorized for up to 60 days but can be extended. A PI may normally be authorized for six months, but also can be extended. A FF investigation has no time limit. A PI should be transitioned into a FF investigation when there is a preponderance of evidence that the original allegation or report is true or when information of a more serious nature is developed.

(U) Finding A

(U) The Army is following Executive Order 12333, Current DoD and U.S. Army Regulations for Conducting Continental United States Counterintelligence Investigative Activity and Evidence Handling Procedures

(U) CONUS CI Investigative Activities

(U) We reviewed 55 CONUS LCAs, PIs, and FF Investigations and found the Army followed Executive Order 12333, DoD Policy, and U.S. Army regulations. (See Appendix A Table 1)

(U/~~FOUO~~) Per AR 381-20 "The Army Counterintelligence Program," CI investigations are conducted to:

(1) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(2) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(3) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(4) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(5) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(6) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(7) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(8) (U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(U/~~FOUO~~) Army CI investigations must always be conducted using appropriate legal standards and in a manner that would not jeopardize the potential for prosecution. Agents conducting CI investigations must be qualified, possess Army intelligence badges and credentials, and be knowledgeable of the elements of proof for national security crimes as established in the Uniform Code of Military Justice and Title 18, United States Code. CI investigations must produce findings, which are accurate, concise, objective, and admissible in a court of law.

(U/~~FOUO~~) To determine if applicable policies and regulations were followed, we reviewed the following documents required by AR 381-20 for LCAs, PIs and FFs: (1) Counterintelligence Incident Reports; (2) Referrals; (3) Authorizations and opening memoranda; (4) Investigative plans; (5) Procedure approvals; (6) Records checks; (7) Banking record requests; (8) Subject interview proposals; (9) extension authorizations; (10) Evidence custody documents; and evidence storage facilities.

(U/~~FOUO~~) **Counterintelligence Incident Reporting.** According to AR 381-12, "Threat Awareness and Reporting Program," Chapter 5, Army CI agents are required to notify the appropriate CI coordinating authority about reportable CI incidents through a Counterintelligence Incident Report. The CI coordinating authority determines if the reported incident warrants a CI investigation. If the information documented in the Counterintelligence Incident Report merits further investigation, the CI personnel responsible for submitting the report are instructed to open an LCA, PI or FF. We

(U/~~FOUO~~) reviewed the LCAs, PIs and FFs and determined that the Counterintelligence Incident Report process, as outlined in AR 381-12, was followed to initiate CI investigations. (See Appendix C)

(U/~~FOUO~~) **Referrals.** Army CI personnel are authorized by AR 381-20 "The Army Counterintelligence Program," Chapter 4 to initiate CI investigations based upon referrals of information from other intelligence and law enforcement agencies. We found that Army CI investigations initiated from referrals of information by outside intelligence and law enforcement agencies were properly documented.

(U/~~FOUO~~) **Authorizations and Opening Memoranda.** In accordance with AR 381-20, Chapter 4, CI investigations must be properly authorized by appropriate Army CI personnel. An LCA may only be authorized by a CI Special Agent in the grades of O-3, Chief Warrant Officer 3, or a civilian pay grade of GG-13 or above with duty as a commander, operations officer or special agent in charge of CI unit with an investigative mission. A CONUS PI may only be authorized by the ACICA, CONUS CICA, or commander of the 902nd MI Group. A CONUS FF may only be authorized by the ACICA. All of the cases we reviewed were initiated by the authorized CI authorities and had the appropriate opening memoranda.

(U/~~FOUO~~) **Investigative Plans.** Investigative plans, according to AR 381-20, Chapter 4, are blueprints for CI investigations and will be used to describe the purpose and objectives of an investigation. The regulation stipulates that investigative plans should be prepared for every FF. The regulation does not state that investigative plans are necessary for LCAs or PIs. Our review of cases disclosed that investigative plans were completed for the FF investigations. We also found that investigative plans were prepared for some LCAs and PIs. Although not required by regulations for an LCA or PI, an investigative plan is a good management tool for all levels of CI investigations.

(U/~~FOUO~~) **Procedure Approvals.** Special investigative procedures specific to CI investigations are outlined in DoD 5240.01-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," and AR 381-10, "U.S. Army Intelligence Activities." A CI special agent conducting an LCA can perform limited investigative activities to include basic records checks, interview sources of information and identify additional leads. During an LCA, the CI agent may not collect and retain physical evidence that requires any approvals that are specified in AR 381-10 and subject interviews can't be done unless approved by the ACICA. Procedure 6, ARMY INSCOM; (b) (3), 50 USC § 3024(i) These procedures must be approved by appropriate CI authorities and legal staff before utilization. Our review disclosed that the special investigative procedures were not conducted without the approval of the appropriate CI authorities and legal staff and were documented accordingly.

(U/~~FOUO~~) **Records Check.** CI special agents are permitted by AR 381-20, Chapter 4 to conduct record checks of local, state, and federal law enforcement and intelligence agencies as well as Army files for LCAs, PIs and FFs. The CI agents may, with approvals from appropriate authorities, request and receive banking records and information from consumer reporting agencies. During our review we found that Army CI agents were conducting appropriate records checks and observing proper procedures for requesting and obtaining financial records.

(U/~~FOUO~~) **Subject Interview Proposals.** Subject interview proposals are required by AR 381-20, Chapter 4. Subject interviews by Army CI agents must be approved by the ACICA. Prior to approval, the CI agent submits a subject interview proposal. The proposal is reviewed by the appropriate legal staff and then submitted to the ACICA for approval. We found that the investigations where subject interviews were done or about to be conducted, the proposal was approved or submitted for approval in accordance with AR 381-20 requirements.

(U/~~FOUO~~) **Extension Authorizations.** As stated earlier, the LCA and PI have time limits for completion. According to AR 381-20, Chapter 4, an LCA may be opened for 60 days. After 60 days an extension must be submitted and approved by either the CICA or the ACICA. The PI has a six month time limit. If more time is needed to resolve the investigation, an extension is granted by the ACICA with consultation from the CONUS CICA. We found that LCA and PI extensions were completed in accordance with AR 381-20 and documented in the case file by the either the CICA or ACICA. A FF does not have a time limit.

(U) Evidence Handling Procedures

(U) On February 22, 2013, the U.S. Army issued an updated AR 195-5, "Evidence Procedures." Only U.S. Army law enforcement entities were required to follow those procedures prior to the updated regulation. The new version was expanded to include U.S. Army CI investigations. When we started our evaluation, the 902nd was drafting a standard operating procedure for evidence handling in order to comply with the updated AR 195-5.

(U) **Evidence Custody Documents and Storage Facilities.** During our site visits, we spoke with available primary evidence custodians and examined evidence storage facilities. According to AR 195-5, Chapter 4, CI units must store evidence in accordance with AR 381-20. For CI units, AR 381-20, Chapter 4, states that evidence seized during a CI investigation may be stored in a security container or a secure room authorized for the storage of material up to SECRET. Access to the evidence must be restricted to the primary or alternate evidence custodian. We checked to determine if there was either a security container or room designated to store evidence. We found that the CI units we visited had proper facilities for storing evidence. We also spoke to the evidence custodians to determine if they knew: what their duties and responsibilities were; how to properly mark and store evidence; how to complete DA Form 4137 Evidence/Property Custody documents; if there were valid orders for their evidence custodian appointments; and proper evidence handling procedures. The evidence custodians we interviewed understood their duties and AR 195-5 requirements.

(U) Within the 902nd, [redacted] We reviewed the evidence ledger and DA Form 4137 Evidence/Property Custody documents. According to AR 195-5, Chapter 2, the evidence ledger shows evidence accountability through cross reference with DA Form 4137. The evidence ledger accounts for document numbers assigned to DA Forms 4137 and must be maintained in a bound book. The evidence ledger is prepared with six columns that annotate the Document Number/Date Received; CI Case Control Number; Description of Evidence; Date of Final Disposition; Final Disposition; and Remarks. The DA Form 4137 must be used to inventory and account for seized evidence. The CI agent who first acquires the evidence is responsible for completing the DA Form 4137. We checked to determine if the evidence ledger was maintained in accordance with policy, the DA Forms 4137s were filled out properly and evidence could be cross referenced from the ledger to the DA Form 4137. We found that the CCA evidence ledger was prepared in accordance with AR 195-5 and the DA Forms 4137s were completed properly and could be cross referenced from the ledger.

(U) Conclusion

(U) We determined that CONUS CI investigative activities complied with Executive Order 12333, DoD policy, and U.S. Army regulations

(U) We also found that CONUS CI evidence handling procedures are in accordance with AR 195-5.

(U) Finding B

(U) Subject Information from Limited Counterintelligence Assessments are not Indexed in the Defense Central Index of Investigations

(U) Subject information from Preliminary Investigations (PIs) and Full Field investigations (FFs) are indexed in the Defense Central Index of Investigations (DCII). However, the Army does not index subject information from Limited Counterintelligence Assessments (LCAs) into the DCII because the LCAs are not sent to the Investigative Records Repository. An LCA is a local investigative file that records investigative activity but it is destroyed after one year. If LCA subject information is not indexed in the DCII before destruction, the subject information and any record of the investigative activity is not retrievable for future reference. AR 381-10, "U.S. Army Intelligence Activities," May 3, 2007, Chapters 2 and 3 allow collection and retention of U.S. Persons information, and AR 381-45, "Investigative Records Repository," May 31, 2013, Chapters 1 and 2 authorize investigative files to be sent to the Investigative Records Repository for subject information indexing in the DCII.

(U) Limited Counterintelligence Assessments

(U/~~FOUO~~) The AR 381-20, "The Army Counterintelligence Program" Chapter 4, states that an LCA can be opened upon receipt of information, which indicates a potential foreign intelligence or international threat to determine if the incident or matter is of CI interest. The LCA is the shortest and least intrusive of the investigative activities. The PIs and FF investigations are more thorough permitting case agents to request and use ARMY INSCOM: (b) (3); 50 USC § 3024(i) [redacted] Also, AR 381-20, Chapter 4-9b describes an LCA as "any investigative activity that exceeds 72 hours." LCAs can include ARMY INSCOM: (b) (3); 50 USC § 3024(i) [redacted]

(U/~~FOUO~~) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted] LCAs are often the first level of investigative activity taken and are used to collect information for the purpose of establishing whether the incident or matter is of CI interest. The PIs and FFs, once completed, are forwarded to the Investigative Records Repository where subject information is entered into the DCII. However, the Army does not do so for LCAs ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(U) According to AR 381-10, Chapters 2 and 3, U.S. Army Intelligence is permitted to collect and retain information concerning U.S. Persons. Long term storage of U.S. Persons information is authorized and the Investigative Records Repository is considered a long term records holding area. AR 381-45, Chapter 2 authorizes U.S. Army Intelligence organizations to send investigative files, including investigations of persons, to the Investigative Records Repository for long term retention. At the Investigative Records Repository, the investigative file is reviewed and materials relating to a subject on which there is no existing file will be accessed into the Investigative Records Repository as a new dossier, assigned an identifying number, and entered into the DCII. If subject information is already indexed into the DCII, the DCII will be updated to reflect the addition of new material. Currently, the Army is indexing PIs and FFs investigations in the DCII in accordance with AR 381-10 and AR 381-45 but not indexing LCAs.

(U) The Defense Central Index of Investigations

(U) In February 1966, the DCII was created with the U.S. Army appointed as the executive agent for that program. In 1972, Defense Investigation Service, later named Defense Security Service, became the DCII's executive agent. In 2010, the Deputy Secretary of Defense transferred administrative responsibility for DCII to the Defense Manpower Data Center.

(U) The DCII is defined in 5 U.S.C. 552, 32 CFR298.3 (a):

> (U) The DCII contains reference to investigative records created and held by the DoD components. The records indexed are primarily those prepared by the investigative agencies of the Military departments and Defense Investigation Service, covering criminal, fraud, counterintelligence, and personnel security information. This index also includes security clearance determinations made by the various components of the DoD. Information in the DCII is not usually available to the general public since general release would violate the privacy of individuals whose names are indexed therein.

(U) The DCII is a central repository for investigative records, to include counterintelligence investigative records. The LCA is an Army counterintelligence investigative record as are the PI and FF. Therefore, it is necessary to maintain the LCA investigative file for future reference. During our LCA reviews, we checked subject information against the DCII data base and determined that LCA subject info was not in the DCII. During interviews we were told that LCA subject information was not entered into the DCII because it wasn't required.

(U) The DCII is a central location that is used to index DoD investigative records and is checked by personnel conducting DoD background investigations and security clearance adjudicators. It is important to maintain an accurate reporting history for subjects of all DoD investigative activity and have those records available for review by investigators conducting personnel security investigations for security clearances and by DoD clearance adjudicators who determine an individual's access and suitability to classified information. Indexing LCA subject information into the DCII ensures that subject information is preserved for personnel security investigations and DoD adjudicator review.

(U) Recommendation

(U) Recommendation B.1

(U) We recommend that the Director, U.S. Army Counterintelligence, Human Intelligence, Disclosure and Security (G-2X), authorize sending LCAs to the Investigative Records Repository so subject information from LCAs can be indexed into the DCII as is done with PIs and FF investigations.

(U) United States Army, Office of the Deputy Chief of Staff, G-2

(U) U.S. Army, G-2, agrees with the finding and recommendation. The Army included guidance in the revision of AR 381-20 requiring investigating elements to retire all LCAs in the Investigative Records Repository and submit a Report of Investigation to the Investigative Records Repository within 45 days of completing the LCA. The Investigative Records Repository indexes retired investigations in the DCII. In July, 2015, the U.S. Army Counterintelligence Coordinating Authority issued interim guidance to CI elements Army-wide, implementing the revised policy.

(U) Our Response

(U) The U.S. Army G-2 has addressed our recommendation and no further comments are required.

(U) Other Matters of Interest

(U) When the evaluation team made site visits and conducted interviews, a number of experienced Army CI personnel provided additional matters of interest concerning changes to some counterintelligence policy and investigative processes the personnel thought would promote efficiency. Some of the recommended changes are incongruous with what current regulations and policy permit. Others were not. Overall, interviewees wanted more transparency from management concerning policy changes that effect investigative operations. Specifically, interviewees said that if management requested and considered input concerning investigative policy changes, it could assist with developing better and more efficient investigative policy. We did not perform verification field work on these issues as they were outside the focus of our evaluation. Management is not required to provide comments to this section. These matters of interest were reported to the evaluation team by U.S. Army counterintelligence personnel and we are providing them to management for situational awareness and any action it deems appropriate.

(U) Investigative Processes

(U) Investigative Access Sources

~~(S//NF)~~ According to AR 381-20, "The Army Counterintelligence Program" Chapter 10-2 c. (1), ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c); (b) (3), 50 USC § 3024(i) [redacted]

~~(S//NF)~~ ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c); (b) (3), 50 USC § 3024(i) [redacted] According to AR 381-20, Chapter 10-2b (2) ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c); (b) (3), 50 USC § 3024(i) [redacted]

~~(S//NF)~~ ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c); (b) (3), 50 USC § 3024(i) [redacted]

(U) Procedure 9 Authorizations

(U) As defined in DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," a Procedure 9 is physical surveillance of United States Persons by DoD intelligence components for foreign intelligence and counterintelligence purposes and can be approved by the head of the intelligence component concerned or a designated senior official of the component.

(U) ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(U) Pursuant to AR 381-10, "U.S. Army Intelligence Activities," Chapter 9-5, related to Procedure 9 approvals, with regards to surveillance of U.S. persons within DoD counterintelligence jurisdiction, the 902nd commander could approve a Procedure 9 for the Group if the authority is delegated by the Army G-2. Interviewees stated that a Procedure 9 is the least intrusive of procedures, includes an extensive legal review by the 902nd and are used in PIs, which the 902nd Group commander is authorized to initiate. Although the 902nd Group Commander can authorize the initiation of a PI, ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted] Since the 902nd Group commander has the authority to initiate a PI, those we interviewed ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted]

(U) Local Staff Judge Advocates Could Provide Routine Investigative Support to Field Offices

(U) Pursuant to AR 381-10, "U.S. Army Intelligence Activities," Chapter 1-6a, Commanders will seek legal advice from their supporting U.S. legal advisor for procedures 5-13. Senior CI personnel that we interviewed suggested that a legal review of routine investigative processes such as obtaining e-mails from local servers, search authorizations and affidavits could be referred to local Staff Judge Advocate offices for approval. Local Staff Judge Advocate's offices provide legal support to the U.S. Army Criminal Investigative Command's Special Agents and the installation Provost Marshal. Additionally, interviewees stated that utilizing local Staff Judge Advocates for routine investigative processes would reduce turn-around time and unburden 902nd and INSCOM legal staff for other requirements. However, consideration must be taken to ensure local Staff Judge Advocates have appropriate clearance levels and the sensitivity of CI investigations must be accounted for.

(U) The U.S. Army CI Policy for Obtaining Government E-mails from Defense Information Systems Agency

(U) Interviews disclosed that the ACICA, without warning, issued new investigative guidance for retrieving U.S. Government e-mails from the Defense Information Systems Agency (DISA) enterprise. According to interviewees, the new policy is more stringent and no explanation was provided to the field for the change.

(U) The new ACICA policy letter, "Retrieving Defense Information System Agency Enterprise Email," dated March 6, 2014, directs field agents to create a packet for submission to the local legal office for review and approval. ARMY INSCOM (b) (3), 50 USC § 3024(i)

[redacted]

(U) [redacted] ARMY INSCOM: (b) (3), 50 USC § 3024(i)

(U) [redacted] ARMY INSCOM: (b) (3), 50 USC § 3024(i)

(U) "Resolved" CI Full Field Investigation

(U) AR 381-20, "The Army Counterintelligence Program," Chapter 4-13b, states that one of the requirements for closing a FF investigation is when the original allegation has been "resolved." However, interviewees related that there is no definition or criteria of what "resolved" means and that not properly defining what a "resolved" investigation is could lead to arbitrary or speculative decisions concerning case termination. Interviews disclosed that some investigations are terminated as "resolved" and the allegations are neither refuted nor established as required by Army Regulation 381-20, Chapter 4-2c.

(U) The Special Investigations Detachment

~~(S//NF)~~ [redacted] ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c)

~~(S//NF)~~ ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c) [redacted]

(U) Responsibility for Operational Control of CONUS CI Investigations

(U) According to AR 381-20,"The Army Counterintelligence Program," Chapter 3-2b, the ACICA maintains technical control of Army CI controlled activities, which are those activities requiring enhanced oversight, legal review, and access control because of their potential for abuse, their sensitivity as they relate to national security, and the need for ensuring senior leadership knowledge. They consist of CI investigations, CI source operations (excluding CI force protection source operations), and CI projects. "Technical control" as defined by AR 381-20 "The Army Counterintelligence Program," conveys the authority to ensure complete and proper accounting of CI investigative and operational activities; compliance with established law and policies; quality assurance; interagency coordination at the national level; investigative coordination across theater boundaries; and Army leadership knowledgeability of significant CI activities.

(U) Headquarters, Department of the Army, Army Doctrine Reference Publication 1-02, defines "technical control" as supervision of human intelligence, counterintelligence, and signals intelligence collection tactics, techniques, and procedures. "Technical control" does not interfere with tasking organic human intelligence, counterintelligence, and signals intelligence collection assets; it ensures adherence to existing policies or regulations by providing technical guidance for human intelligence, counterintelligence and signals intelligence tasks within the information collection plan.

(U) "Operational control" as defined by The Army Doctrine Reference Publication, 1-02, is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designing objectives, and giving authoritative direction necessary to accomplish the mission.

(U) [redacted] ARMY INSCOM: (b) (3), 50 USC § 3024(i) [redacted] (See Appendix's B and C.)

Appendix A

(U) Scope and Methodology

(U) We conducted this evaluation from November 26, 2013, through February 12, 2016, in accordance with the "Quality Standards for Inspection and Evaluation" published by the Council of Inspectors General on Integrity and Efficiency in January 2012.

(U) Our objective was to determine whether CONUS U.S. Army CI investigative activities and evidence handling procedures complied with Executive Order 12333, DoD policy and U.S. Army regulations. We worked closely with an experienced Army CI subject matter expert during the course of this evaluation.

(U) To meet our objective, we reviewed U.S. law, DoD and Army regulations and policy to determine current CI investigative activities and evidence handling procedure. We made 18 site visits where we reviewed cases and interviewed leadership and field agents. The site visit locations included all four 308th company headquarters, seven field offices, the Special Investigations Detachment, CCA, Army Operations Security Detachment, and the Army CI Center. We interviewed investigative oversight personnel at the US Army G-2X, ACICA, CONUS CICA, 308th and 310th Battalions. We also met with personnel from the Defense Intelligence Agency, US Army Intelligence Center of Excellence, and the DoDCAF.

(U) We evaluated 55 open CONUS CI LCAs, PI and FF investigations that the 902nd provided upon our request to review cases within the evaluation period. (See table 1.) We evaluated those FFs, PIs and LCAs to determine observance of established administrative and operational procedures. We also evaluated existing case management, investigative processes, and oversight mechanisms for efficiencies.

Appendix B

(S//NF) Table 1. Distribution of Army CI Investigative Activities During Evaluation Period

(S//NF)	CI Investigation Case Category		
Office Designations	Full Field Investigations	Preliminary Investigations	Limited Counterintelligence Assessment

ARMY INSCOM: (b) (1), EO 13526, sec. 1.4(c)

[redacted]

55

(S//NF)

Source: U.S. Army CI Investigations case review

(U) Use of Computer Processed Data

(U) We did not use computer processed data to perform this evaluation.

(U) Prior Coverage

(U) No prior coverage has been conducted on United Stated Army Counterintelligence Investigations and Evidence Handling Procedures in the past five years.

~~(S//NF)~~ ARMY INSCOM (b) (1), EO 13526, sec 1.4(c)

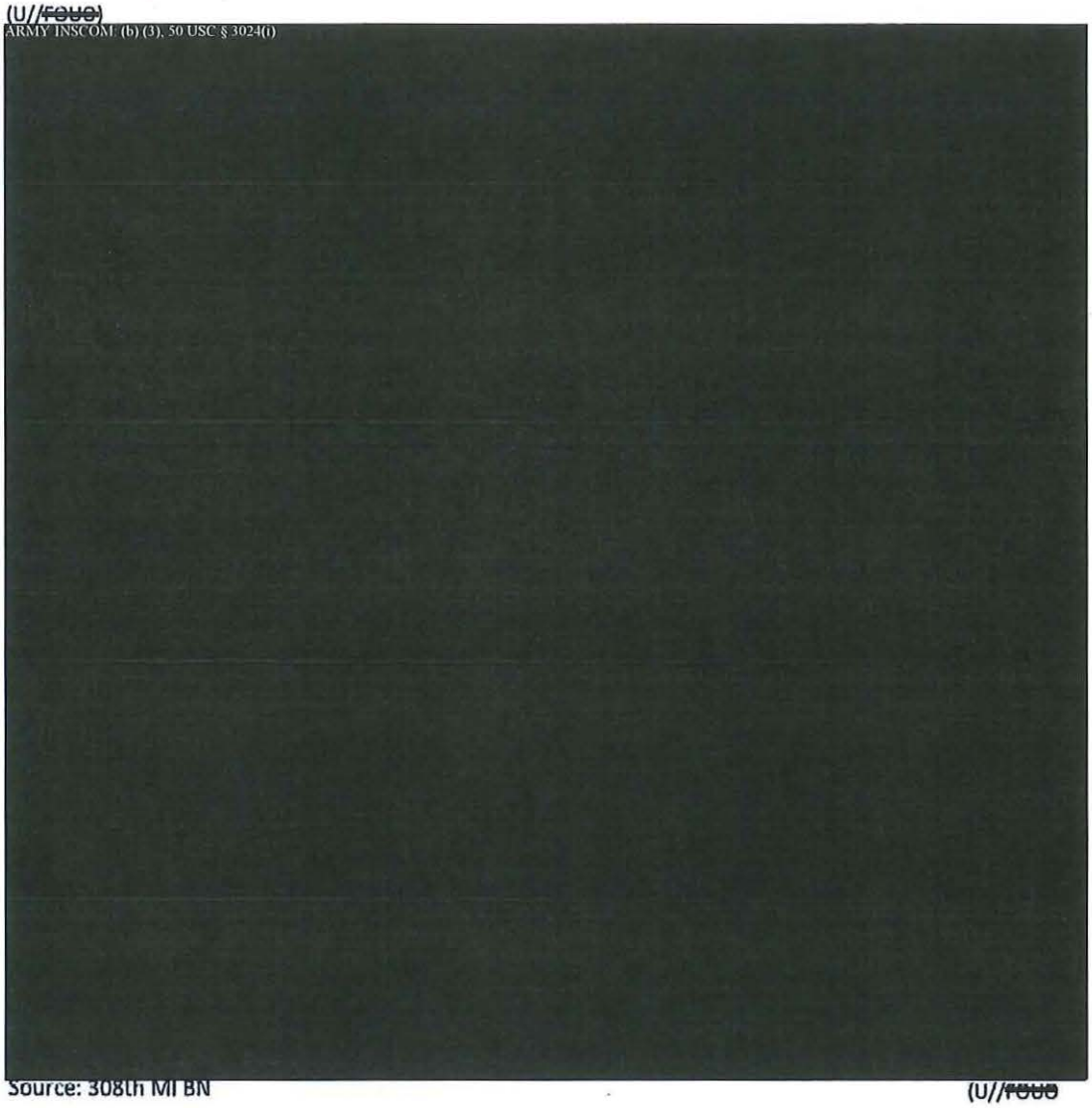
~~(S//NF)~~
ARMY INSCOM (b) (1), EO 13526, sec 1.4(c)

Source: U.S. Army CI Investigations case review ~~(S//NF)~~

(U) Appendix C

(U//~~FOUO~~) US Army CI Investigation Process

(U//~~FOUO~~)
ARMY INSCOM: (b) (3), 50 USC § 3024(i)



Source: 308th MI BN (U//~~FOUO~~)

Management Comments

(U) United States Army, Office of the Deputy Chief of Staff, G-2

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
1000 ARMY PENTAGON
WASHINGTON, DC 20310-1000

JUN 17 2016

DAMI-CDC

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

SUBJECT: (U) Draft Evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures (Project No. D2014-DINT-0069.000)

1. (U) The Army concurs with the finding of the 27 April 2016, Department of Defense (DoD) Inspector General (IG) draft report concerning its evaluation of United States Army Counterintelligence Investigations and Evidence Handling Procedures (Project No. D2014-DINT-0069.000). The DoD IG found that subject information from Limited Counterintelligence (CI) Assessments (LCAs) was not indexed in the Defense Central Index of Investigations (DCII).

2. (U//~~FOUO~~) To address the finding, the Army included guidance in the revision of Army Regulation 381-20, The Army Counterintelligence Program. The guidance requires investigating elements to retire all LCAs in the U.S. Army Investigative Records Repository (IRR) and submit a Report of Investigation (ROI) to the IRR within 45 days of completing the LCAs. The IRR indexes retired investigations in the DCII. This will ensure Army complies with DoD Instruction 5505.07, Titling and Indexing Subjects of Criminal Investigations in the Department of Defense, 27 January 2012. In July 2015, The Army Counterintelligence Coordinating Authority (ACICA) promulgated interim guidance to CI elements Army-wide, implementing the revised policy.

3. (U) The Army conducted a classification review of the IG report and concurs with the SECRET//NOFORN classification.

4. (U) The Office of the Deputy Chief of Staff, G-2 point of contact is DoD OIG: (b) (6) [redacted]

ROBERT P. ASHLEY, JR.
Lieutenant General, GS
Deputy Chief of Staff, G-2

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Acronyms and Abbreviations

(U)

ACICA	US Army Counterintelligence Coordinating Authority
AR	Army Regulation
BN	Battalion
CCA	Cyber Counterintelligence Activity
CI	Counterintelligence
CICA	Counterintelligence Coordinating Authority
CONUS	Continental United States
DCII	Defense Central Index of Investigations
DISA	Defense Information Systems Agency
DoD	US Department of Defense
FF	Full Field
INSCOM	US Army Intelligence and Security Command
LCA	Limited Counterintelligence Assessment
MI	Military Intelligence
PI	Preliminary Investigation

(U)

~~SECRET//NOFORN~~

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

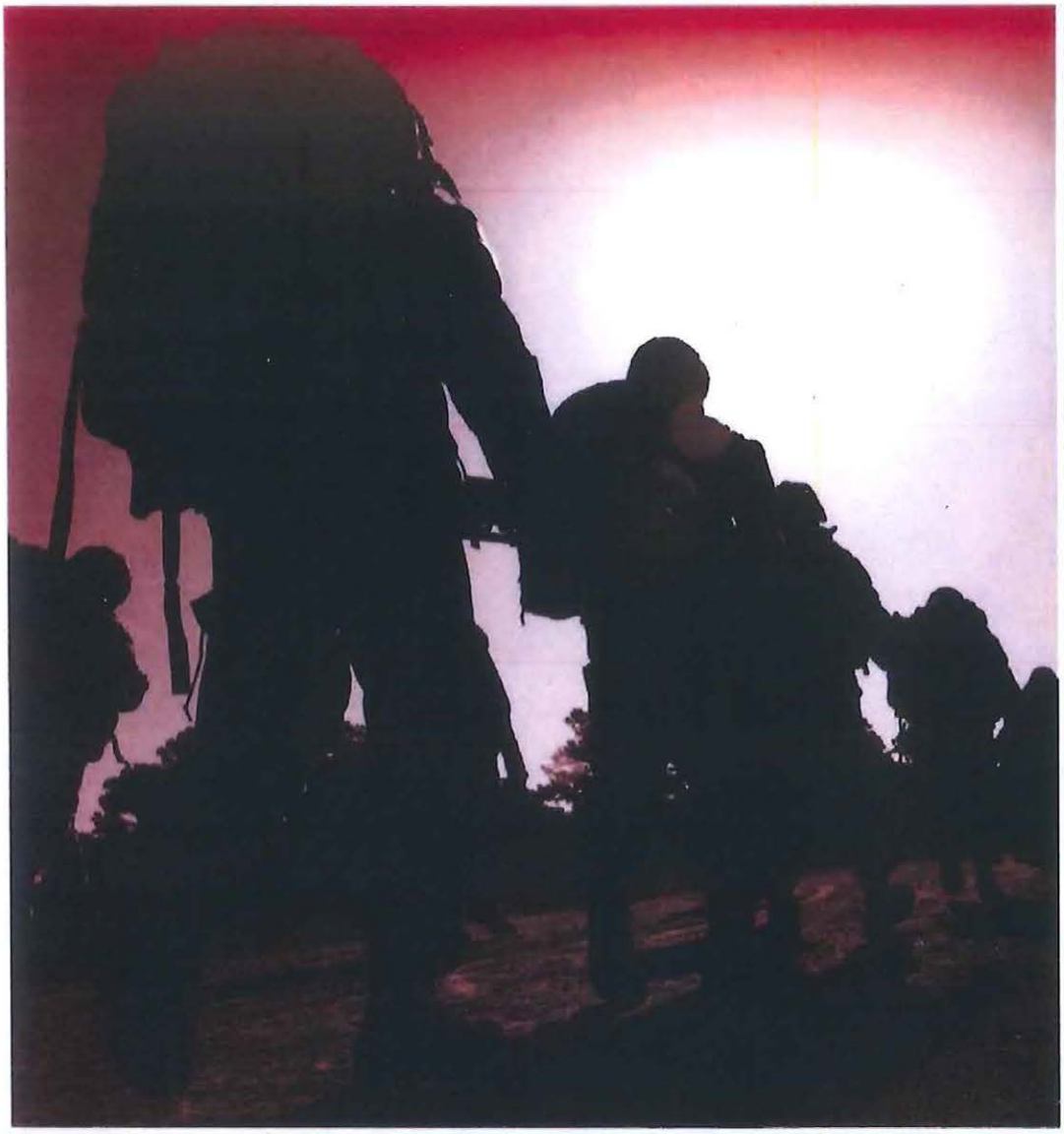
Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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

~~SECRET//NOFORN~~