

CHAPTER 8: TIG CI Office

Section I: Introduction

8-1. Purpose

(U) Establish and describe the roles and functions of the Theater Intelligence Group Counterintelligence (TIG CI) Office. These roles include but are not limited to Counterintelligence (CI), Counterespionage (CE), Threat Awareness Reporting Program (TARP), Military Counterintelligence Collection (MCC), Covering Agent Program (CAP), CI Support to Interrogation Operations, CI Analysis, CI Support to Force Protection.

8-2. Scope of Operations

8-2.1. (U) TIG CI Special Agents (SA) conduct SAEDA investigations to identify, neutralize, and/or exploit the Adversarial, Terrorist, or Foreign Intelligence Security Service (FISS) threat to the Detention Facility in Parwan (DFIP) and its personnel, mission, and operations. TIG CI will report SAEDA incidents pertaining to threats to the DFIP, IAW Chapter 3, AR 381-12, through the United States Forces – Afghanistan (USFOR-A) Task Force Counterintelligence Coordinating Authority (TFCICA) and subsequently to the 513th Theater Counterintelligence Coordinating Authority (TCICA).

8-2.2. (U) TIG CI will support interrogation operations by providing assistance to the Interrogation Coordination Element (ICE), the Strategic Debriefing Center (SDC), and the CI mission throughout Afghanistan by submitting Source Directed Requirements (SDR) and/or conducting CI interviews of detainees of CI Interest to answer CI collection requirements and Priority Intelligence Requirements (PIR).

8-2.3. (U) TIG CI shall conduct MCC to obtain information in support of efforts to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on the behalf of foreign powers; organizations; persons or their agents; or international terrorist organizations or activities, as well as to generate leads for CI investigations and operations.

8-2.4. (U) TIG CI shall implement a Covering Agent Program (CAP) which will assign a primary supporting SA to each command, agency, and section within the DFIP. The CAP will ensure detailed familiarity with the supported element's operations, personnel, security, and vulnerabilities, and in turn provide the element with a designated point of contact for reporting matters of actual or potential CI interest.

8-2.5. (U) TIG CI Analysts will process all information related to detainees of CI interest as it pertains to espionage or other foreign intelligence activities, sabotage, terrorism, and other related threats to the DFIP and Coalition Forces (CF) in order to develop CI products for dissemination. TIG CI analytical products will support the TIG Commander, CI/CE investigations, MCC operations, and/or the overall CI mission in Afghanistan.

8-2.6. (U) TIG CI is direct support to the TIG and general support to the DFIP. TIG CI SAs provide a direct link to the TIG J2 in Force Protection and Camp security matters. The TIG J2 sends requests for information (RFI's) and requests for action (RFA's), but does not task TIG CI. Tasking authority is limited to the United States Forces – Afghanistan (USFOR-A) Task Force Counterintelligence Coordinating Authority (TFCICA), TIG Commander and the TIG J3 and routed through the Counterintelligence Staff Officer (CISO) or the TIG CI Special Agent in Charge.

8-2.7. (U) Provide direct CI support to the TIG and general CI support to the DFIP to detect, deny, neutralize, and/or exploit intelligence collection efforts against DFIP facilities, operations, and personnel. TIG CI will accomplish this mission by providing the following capabilities:

8-2.7.A. (U) Covering Agent Program

8-2.7.B. (U) SAEDA

8-2.7.C. (U) MCC

8-2.7.D. (U) CI Analysis

8-2.7.E. (U) CI Support to Interrogation Operations

8-2.7.F. (U) CI Support to Operation Third Wheel

8-2.7.G. (U) CI Support to CM&D

8-3. References

a. (U) AR 381-10

b. (U) AR 381-12

c. (U) AR 381-20

d. (U) AR 381-172 (~~S//NF~~)

e. (U) AR 381-47 (~~S~~)

f. (U) AR 381-141 (~~C~~)

g. (U) FM 2-22.2

h. (U) DOD 5240.1R

i. (U) JP 2-01.2 (~~S//NF~~)

j. (U) DCID 5/1 (~~S~~)

k. (U) DIAM 58-11 (~~S//NF/LIMDIS~~)

l. (U) Executive Order 12333

m. (U) DOD 5240.2

Section II: Duties and Responsibilities

8-4. Jurisdiction

8-4.1. (U) US Army CI SAs assigned, attached, or under the operational control of TIG CI have CI investigative and operational jurisdiction over the individuals outlined below, who are OCONUS and are physically located within Afghanistan; specifically on the DFIP facility compound:

8-4.1.A. (U) US Army personnel on active duty and their family members.

8-4.1.B. (U) Army National Guard and U.S. Army Reserve personnel operating at JIDC.

8-4.1.C. (U) Current DA civilian employees, including foreign national employees and their family members.

8-4.1.D. (U) Army contractors and their family members, subject to coordination with the FBI, CIA, and host government agencies.

8-4.1.E. (U) Retired Army personnel, Reserve Components personnel and other US persons, subject to coordination with the FBI, CIA, and host government agencies.

8-4.1.F. (U) Foreign nationals who are applicants for Department of Defense (DoD) employment, are DoD employees, or are former DoD employees, no matter whether they have,

require, or had access to US classified information, unless responsibility is otherwise assigned by US law, executive directive, or agreement with the host government.

8-4.1.G. (U) Foreign nationals not affiliated with the DoD, subject to coordination with the CIA and agreements with the FBI, other US Government intelligence components and host nation governments. These investigations are under the auspices of Status of Forces Agreements (SOFA) and may be designated bi-lateral investigations.

8-4.1.H. (U) Active, retired, and reserve component personnel of other services, DoD civilian employees and family members, and DoD foreign nationals, where DoD has given Army CI geographic jurisdiction.

8-5 TIG CI Priorities of Work

8-5.1. (U) Conduct CI investigations when an attempt is made to penetrate DFIP facilities or exploit DFIP personnel, to include TIG facilities and personnel.

8-5.2. (U) Provide Counterintelligence Support to Interrogation Operations.

8-5.3. (U) Conduct the Covering Agent Program (CAP).

8-5.4. (U) Conducting MCC operations only when in relation to the DFIP priorities.

8-5.5. (U) Exchanging information with the Interrogation Control Element (ICE) and Strategic Debriefing Center (SDC).

8-5.6. (U) Liaising with Military Police, DFIP personnel, COIN personnel and other Intelligence personnel.

8-5.7. (U) Monitor specific interrogations, as requested by the ICE and the SDC for CI related information.

8-5.8. (U) Push CI reporting to the Fusion Analysis Cell for fusion with ICE and SDC HUMINT reporting.

8-5.9. (U) Provide CI advice to interrogators.

8-5.10. (U) Further identify counterintelligence issues within in the detainee population.

8-5.11. (U) Exchange Force Protection-related information gathered under priorities of work 1 & 2.

8-5.12. (U) Provide TARP awareness expertise to leaders.

8-5.13. (U) Conduct unit level TARP awareness briefings IAW the Bi-annual requirement.

8-5.14. (U) Assist the Military Police in stopping the information flow from the detainee population to ACF outside the detainee population.

8-5.15. (U) Coordinate with TCICA concerning CI investigations when an attempt is made to penetrate DFIP facilities or exploit DFIP personnel.

8-5.16. (U) Spot and assess potential sources for MCC Operations.

8-6. TIG CI field office Individual Responsibilities

8-6.1. (U) Provide Collection and operational focus for CI teams.

8-6.2. (U) Prepares, reviews, and approves investigative/operational reports of investigations and inspections.

8-6.3. (U) Oversees the terrorism counteraction analysis and threat analysis.

8-6.4. (U) Investigates national security crimes of CI interest as defined by applicable regulations and U.S. Code.

8-6.5. (U) Conducts and supervises both overt and covert investigations.

8-6.6. (U) Supervises the technical performance of subordinate military and civilian personnel in related job skills.

8-6.7. (U) Develops and approves investigative plans before dissemination to the USFOR-A TFCICA and the TCICA.

8-6.8. (U) Represents the Army's interests in investigations conducted collaterally with other organizations.

8-6.9. (U) Establishes the agent and analyst teams, concepts, products, and operations.

8-6.10. (U) Ensures all agents and analysts are qualified for their assigned duty positions and responsibilities.

8-6.11. (U) Acts as a conduit between TIG CI and the DFIP.

8-7. Operations Officer

8-7.1. (U) The Operations Officer is responsible for the overall collections focus and dissemination of reporting from the CI Team. The Operations Officer has the following duties:

8-7.1.A. (U) Provides the collection and operational focus for CI teams.

8-7.1.B. (U) Provides quality control and dissemination of reports.

8-7.1.C. (U) Assists in mission analysis for the supported commander.

8-6.1.D. (U) Acts as a conduit between CI team and the JIDC.

8-6.1.E. (U) Integrates the CI team support into JIDC interrogation operations.

8-8. Assistant Special Agent In Charge (ASAIC)

(U) The ASAIC is the second in command and is responsible for assuming all the above SAIC appointed responsibilities in their absence. The ASAIC is also responsible for supporting the SAIC with the daily duties and obligations of TIG CI.

8-9. Special Agent (SA)

(U) The SAs are responsible for conducting all missions, operations, investigations and reporting to the SAIC/ASAIC IAW the regulations and policies set forth.

8-10. CI Analysts

(U) Responsible for providing intelligence research and production in support of TIG CI's mission. TIG CI analysts will monitor and update existing CI Collection Requirements and Emphasis Messages; they also must be proficient with intelligence databases such as Combined Information Data Network Exchange (CIDNE), Pathfinder, Query Tree, ARCGIS, Biometrics Automated Toolset (BATS), Cell phone Exploitation (CELLEX), and Detainee Information Management System (DIMS) systems. TIG CI analysts will process all source information concerning espionage or other foreign intelligence activities, sabotage, terrorism, and other related threats to the DFIP, its personnel and CF to develop CI products for dissemination. TIG CI Analytical products will support the TIG Commander, CI/CE investigations, MCC operations, and/or other US Military Commanders.

8-11. Interpreter

(U) TIG CI requires a Category II (CAT II) linguist for daily functions. The interpreter must be able to translate Pashtu and Dari. The linguist must understand their job will require them to work unpredictable hours in support of TIG CI operational requirements.

8-12. CI Support to the Interrogation Elements:

8-12.1. (U) TIG CI provides direct and indirect support to the Interrogation Elements (ICE and SDC):

8-12.1.A. (U) Agents support the Interrogation elements by providing CI assistance in the interrogation booth.

Agents listen to select interrogations to screen for anything of force protection value and assist interrogators by providing a list of follow up questions if the interrogation is deemed to be of CI interest. Agents are also able to utilize their source pool to assist interrogators in answering any questions on individuals deemed of interest that are not currently detained. Sources assist in corroborating or negating a detainee's story to assist interrogators with a determination in the detainee's honesty during an interrogation.

8-12.1.B. (U) Analysts within TIG CI support analysts within the Interrogation Elements by assisting in research through the CI channels. Analysts have the ability to produce questions to pass to agents for a source that has been identified as having placement and access to the information being provided by a detainee; agents are not required to use questions produced by the analyst. Since the information may be outdated due to the amount of time a detainee has been held within the facility, TIG CI analysts may be able to provide more recent information gathered from sources.

8-12.1.C. (U) TIG CI may provide the ICE and the SDC with a detainee packet complete with a sworn statement provided by a TIG CI coded Source. This allows ICE interrogators and analysts more background information to research prior to entering into an interrogation with a detainee detained by TIG CI.

8-12.2. (U) CI Support to the FAC: TIG CI supports the FAC by providing another channel of reporting to assist in the overall collection of intelligence. The FAC is able to combine the information gathered from interrogations and TIG CI to put together comprehensive analysis.

8-13. TIG CI Interactions with the TIG

8-13.1. (U) Interaction with TIG Operations: TIG Operations acts as the administrative conduit for all documentation requiring command signatures. TIG Operations assists TIG CI in coordinating with units of action, approving ICF documentation, approving Rewards Program documentation, and submitting convoy requests.

8-13.2. (U) Interaction with the TIG Collection and Management Division (CM&D): CM&D acts as the conduit for all operational reporting. They provide quality control of TIG CI IIRs and SPOT Reports. CM&D publishes intelligence reports originating from TIG CI. CM&D has a Reports Officer designated to publish TIG CI intelligence information. CM&D also provides collection requirements to TIG CI, and notifies TIG CI of any evaluations on TIG CI reports.

8-13.3. (U) Interaction with the JIDC Polygraph: Polygraph exams are a valuable asset to TIG CI. They give Agents the ability to substantiate information and vet sources.

8-14. TIG CI Liaison Activities

8-14.1. (U) TIG CI routinely liaises with the following personnel/units:

8-14.1.A. (U) TIG J2: The TIG J-2 is responsible for providing the TIG Commander with intelligence assessments based in part on recommendations from the Field Office. TIG CI works closely with the JIDC J-2 to assist in force protection. TIG CI provides support by conducting Threat Vulnerability Assessments (TVA) and passing any relevant force protection information to the LSA J-2 via SPOT Reports, monitoring detainee activities; providing recommendations of personnel detained as a possible threat to Coalition Forces based on interviews/screenings.

8-14.1.B. (U) Badge/Access Control: The LSA Commander issues all JIDC badges and determines the level of access granted with assistance from the J-2. TIG CI also provides

recommendations to the Badge/Access Control sections of any personnel that need to have their JIDC access reviewed or revoked based on information gathered by TIG CI from walk-in interviews.

8-14.1.C. (U) MP BDE/BN: The MP BDE/BN conducts detention facility operations at the JIDC Internment Facility in support of its MP BDE in order to maintain custody, control, and care of detainees IAW the Geneva Convention and Army regulations. TIG CI maintains a direct line of communication with the MP S2, MP S3, and COIN team. When necessary, TIG CI will brief the MP Commander directly on issues that directly impact his/her command.

8-14.1.C.1. (U) Detainee Facility: The MPs are responsible for the overall care and order of the detainee facility and the detainees within the JIDC. The MP S2 informs TIG CI of all detainee-related force protection concerns. TIG CI analysts correlate the detainee information to other force protection information gathered.

8-14.1.D. (U) Perimeter/Tower Guards: Task Force Protector provides guards for the towers. The guards provide source operations assistance to TIG CI by providing a safeguard for the entrance and exit of sources to reception at ECP 4. TIG CI SAs interact with the reception guards on a regular basis. TIG CI coordinates with the reception guards referencing appropriate actions involving walk-in. As necessary, TIG CI administers Secrecy Affirmation Statements to all guards that have visibility to TIG CI Source Operations.

8-14.1.F. (U) Criminal Investigative Command (CID): CID ensures that known or suspected serious crimes and crimes which may result in damaging the public confidence in the Army are investigated. CID participates in the Army crime prevention program by identifying areas which are especially vulnerable to crime and by making recommendations to appropriate authorities for elimination of conditions conducive to criminal activity. CID will investigate and deter major procurement and contract fraud. CID investigates crimes in sensitive Army programs, computer crime and areas of special interest. CID protects designated DOD officials. CID investigates all reports of detainee abuse in the DFIP. TIG CI and CID share information that falls in the scope of one another's office. TIG CI and CID work jointly on cases that are of both MI value and of criminal interest after coordination and approval from SCOSWA.

8-14.1.G. (U) Camp Sabalu-Harrison Base Defense Operations Center (BDOC): BDOC is responsible for the security of U.S. and Coalition Military Facilities located on Camp Sabalu-Harrison. TIG CI to coordinates with BDOC for Force Protection on the LSA.

8-15. CARP

(U) The Counterintelligence Threat Awareness and Reporting Program establishes policy, responsibilities, and procedures for the recognition and prompt reporting of incidents of attempted or actual espionage, subversion, sabotage, and terrorism directed against the U.S. Army and its personnel; of illegal diversion of technology; unauthorized intrusion into automated information systems; unauthorized disclosure of classified information; and other incidents of a CI nature. The Army's program for CI awareness, education, and reporting is still known collectively as SAEDA. The goal of TARP program is to secure the assistance of every DA member in the deterrence and detection of intelligence and terrorist threats to the Army. The US Army SAEDA program is the reporting of incidents that meet the criteria as defined by AR 381-12. A US Army Intelligence (USAI) investigation may be initiated IAW AR 381-47 (S) and AR 381-20 based upon a Counterintelligence Incident report but this is not the primary purpose of the program. The program is a reporting venue for SAEDA incidents.

8-16. BATS Alerts

(U) Visitors entering VBC through ECP 4 are checked for BATS entries. If an individual come up with an Alert in BATS, the guard force notifies the MP TOC and BDOC who in turn notifies TIG CI. TIG CI will look at the information provided in BATS and make a determination if a SA should be dispatched to interview the individual based on CI nature. If it is determined that there is no CI nature, TIG CI has no actions. If a CI nature is determined, TIG CI will notify the ADOC of their intent to question the individual.

8-17. Regulations

8-17.1. (U) AR 381-10 US ARMY INTELLIGENCE ACTIVITIES (Unclassified).

This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons. It implements DoD Directive 5240.1, and replaces the November 30, 1979 version of DoD Regulation 5240.1-R. It is applicable to all DoD intelligence components.

8-17.2. (U) AR 381-12 SUBVERSION AND ESPIONAGE DIRECTED AGAINST THE U.S. ARMY (SAEDA) (Unclassified). This regulation establishes policy, responsibilities, and procedures for the recognition and prompt reporting of incidents of attempted or actual espionage, subversion, sabotage, and terrorism directed against the U.S. Army and its personnel; of illegal diversion of technology; unauthorized intrusion into automated information systems; unauthorized disclosure of classified information; and other incidents of a CI nature. This regulation establishes the requirement for CI awareness and education. The Army's program for CI awareness, education, and reporting is known collectively as SAEDA.

8-17.3. (U) AR 381-14 TECHNICAL COUNTERINTELLIGENCE (TCU) (~~CONFIDENTIAL~~) This regulation is a consolidation of AR 381-14 (S) and AR 380-19-1 (~~C~~) to cover the control of compromising emanations (TEMPEST) and technical surveillance countermeasures.

8-17.4. (U) AR 381-141 INTELLIGENCE CONTINGENCY FUNDS (ICF) (~~CONFIDENTIAL~~) This regulation establishes uniform procedures for the use, administration, supervision and control of intelligence contingency funds.

8-17.5. (U) AR 381-172 COUNTERINTELLIGENCE FORCE PROTECTION SOURCE OPERATIONS (CFSO) and LOW LEVEL SOURCE OPERATIONS (LLSO) (~~SECRET/NOFORN/NOINTEL~~). This regulation establishes the authority and responsibility for counterintelligence source protection operations. It includes guidance on the definition, conduct of, responsibilities, and approval authority over such activities.

8-17.6. (U) AR 381-20 THE ARMY COUNTERINTELLIGENCE PROGRAM (Unclassified) This regulation sets forth the policy, responsibilities, jurisdictions and procedures for the Army CI Program.

8-17.7. (U) USAREUR Regulation 381-22 PROCESSING WALK-INS (Unclassified) This regulation pertains to handling and processing walk-ins of intelligence interest. This regulation applies to USAREUR units and the 66th Military Intelligence Group (Provisional).

8-17.8. (U) AR 381-47 U.S. ARMY COUNTERESPIONAGE ACTIVITIES (~~SECRET~~) This regulation is a consolidation of AR 381-47 and AR 380-12-1. It establishes the authority and responsibility for the conduct of United States Army CE activities.

8-17.9. (U) AR 381-102 U.S. Army Cover Support Program (~~CONFIDENTIAL~~)

8-17.10. (U) FM 2-22.2 Counterintelligence (Unclassified)

8-17.11. (U) FM 34-60A Counterintelligence Operations (~~SECRET~~)

8-17.12. (U) DOD 5240.1R Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons (Unclassified)

8-17.13. (U) JP 2-01.2 Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Joint Operations (~~SECRET/NOFORN~~)

8-17.14. (U) DCID 5/1 Espionage and Counterintelligence Activities Abroad (~~SECRET~~)

8-17.15. (U) DIAM 58-11 Department of Defense HUMINT Policies and Procedures