BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE TACTICS, TECHNICQUES
3-10.3

14 MAY 2021

Tactical Doctrine

COUNTERINTELLIGENCE SUPPORT TO FORCE PROTECTION IN OVERSEAS CONTINGENCY OPERATIONS

ACCESSIBILITY: Publications and forms are available on the e-publishing website at **www.e-publishing.af.mil** for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/IGX

Certified by: SAF/IG
(Lt Gen Sami D. Said)

Supersedes: AFTTP 3-10.3, 25 August 2015

Pages: 14

This Air Force Tactics, Techniques, and Procedures (AFTTP) describes the activities the Air Force Office of Special Investigations (AFOSI) employs in support of AFPD 31-1, *Integrated Defense*. AFOSI conducts investigations, operations, and counterintelligence (CI) collection activities to find, fix, track, and neutralize adversary threats to enable Department of the Air Force operations. This AFTTP describes command and organizational relationships, execution using functional capabilities, and training requirements to conduct effective CI support to force protection (CISFP). While these TTP principles are focused on expeditionary operations in high threat locations, the tactical doctrine principles remain the same for home-station operations. This AFTTP applies to civilian employees and uniformed members of the Department of the Air Force, the Air Force Reserve, and the Air National Guard. The doctrine prescribed in this document is authoritative, but not directive. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed of in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate career field functional manager's chain of command. This publication may be supplemented at any level, but all Supplements must be routed to the OPR of this publication for coordination prior to certification and approval.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include realigning counterthreat operations under the broader concept of CISFP; reflecting language in updated Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations* and joint publications; and redefining how Tactical Security Elements fall within the deployed chain of command.

Chapter 1

COUNTERINTELLIGENCE SUPPORT TO FORCE PROTECTION OVERVIEW

1.1. Overview. AFMD 39, *Air Force Office of Special Investigations,* directs AFOSI, a federal law enforcement and CI agency and combat-ready military organization, to provide the Department of the Air Force (DAF) a wartime CI capability. AFOSI conducts operations in hostile, uncertain, and permissive environments, throughout multiple domains, to protect the designated vital interests of the DAF, Department of Defense (DoD), and U.S. Government from adversary threats. Adversary threats include terrorists, insider threats, foreign intelligence entities, criminals, and enemy forces. AFOSI, utilizing concurrent law enforcement and CI authorities, neutralizes threats with appropriate interagency, joint, and combined forces, primarily through CISFP.

1.2. CISFP. CISFP is the employment of AFOSI capabilities in support of friendly force protection efforts. Force protection includes offensive and defensive preventive measures taken to mitigate hostile actions against personnel, resources, facilities, and critical information. AFOSI operates inside and outside of established base perimeters and is the DAF lead for identifying, locating, and tracking adversaries threatening U.S. and allied personnel, resources, facilities, and critical information. CISFP provides commanders situational awareness, drives force protection condition changes, and forewarns of possible attacks. AFOSI conducts the following activities in support of FP: CI investigations and operations; offensive CI operations; CI collection activities, such as military CI collections (MCC), liaison, threat briefings, tactical debriefings, field interviews, and tactical questioning; site exploitation; surveillance, counter surveillance, and surveillance detection; protective service operations; CI activities in cyberspace; threat assessments and analysis; and CI functional services, such as technical services, technical surveillance countermeasures, polygraph, and credibility assessments.

1.3. Counterthreat Operations. As a subset of CISFP, AFOSI executes Counterthreat Operations (CTO) in hostile and uncertain environments to find, fix, track, neutralize, and assess threats in order to create a sustained permissive environment for air, space, and cyberspace operations. Threats to active airfields may extend far beyond the area designated as a base boundary, including aircraft approach and departure corridors and indirect fire attacks to taxiing and parked aircraft. To address these threats, the air component uses the base security zone construct to plan for and consider the ground threats and hazards that could affect airfield operations. AFOSI CTO supports these efforts by seamlessly collecting, fusing, and disseminating intelligence on threats to the base security zone from a broad array of sources on a continual basis.

1.3.1. CTO utilizes intelligence-driven operations employing information derived from multiple intelligence and CI sources. Successful CTO requires deliberate collaboration, coordination, and deconfliction between AFOSI personnel and entities of various U.S. and foreign partner agencies. A whole-of-government and interservice approach, coupled with partnerships from host nation law enforcement and intelligence services, will effectively neutralize threats and foster DAF interests. AFOSI executes CTO by integrating all AFOSI capabilities into the Air Force "kill chain" cycle (find, fix, track, neutralize, and assess) to achieve the desired effects. In joint or coalition environments, AFOSI integrates its capabilities into joint, coalition, or host-nation “kill chain” processes. CTO tactical doctrine is a compilation of knowledge and expertise and describes the appropriate AFOSI role in integrated

defense (ID) in hostile and uncertain environments. In permissive environments and in friendly foreign countries, AFOSI executes CISFP in accordance with AFOSI Instruction, 71-144, Volume 1, *Execution of AFOSI's Counterintelligence Mission*.

1.4. CISFP Planning. CISFP supports military operations by providing threat information to commanders at all levels, from combatant commands to subordinate joint forces. Commanders depend on timely, accurate threat information and intelligence, including the adversary's disposition, tactics, intent, and capabilities, to inform their decision-making processes and better understand the operational environment (OE). AFOSI units should develop CISFP plans focused on providing the commander with the intelligence required to create desired effects and achieve operational objectives.

1.4.1. CISFP plans must take into account the relevant, local aspects of the OE, such as the adversary and other actors, and factors such as political, military, economic, social, information, and infrastructure systems. CISFP plans consist of, but are not limited to, a unit's mission, map layout illustrating the base security zone, areas of concern/areas of influence, focused collection requirements, identified threats, and potential adversary courses of action.

1.4.2. When planning CTO, the friendly freedom of maneuver along with adversary capability and intent, in the base security zone, must be considered when assessing how any outside-the-wire actions will be executed. AFOSI should only conduct unilateral CTO activities in a hostile environment when U.S./coalition forces are assessed as dominating the ground defense area. When US/coalition forces do not dominate the ground defense area, AFOSI senior leaders and supported commanders must assess the minimum enabler capabilities required to mitigate risk for any outside-the-wire activity by AFOSI members. If requisite enablers are not in place, AFOSI personnel should only operate as part of larger maneuver units.

1.5. CISFP Training. Executing successful CISFP requires training and familiarity in multiple CI disciplines, working with interagency and coalition partners, and diplomacy. Additionally, due to the inherent danger of CTO missions, all effort should be made to maximize training. Effective ground combat skills are imperative to survival in hostile, highly contested, or uncertain environments with degraded communications. Initial and recurring field training on perishable skills is vital and should be conducted both in pre-deployment and in theater. Refer to **Attachment 2** for examples of skills on which AFOSI agents and analysts should be trained prior to conducting CTO. Refer to Reading List**,** **Attachment 3** for additional references and resources to be more familiar with the CISFP mission and guidance.

1.5.1. The United States Air Force Special Investigations Academy Counter Threat Operations Course trains AFOSI agents in realistic scenarios to perform in high-risk locations more efficiently and effectively. This training is a team-centered, operationally intense, execution-based immersion course designed to train agents in core tactical skills. Curriculum focuses on perishable skill sets used in hostile or non-permissive environments. Prior to a contingency deployment or assignment, all military and civilian AFOSI personnel are required to attend mandatory advanced training, in accordance with AFI 10-403_AFOSISUP, *Deployment Planning and Execution*.

1.5.2. AFOSI agents conducting CTO should conduct formal pre-mission briefings, rehearsals of concept drills, and post-mission debriefings. Mission briefings should, at a minimum, include any foreign and domestic mission participants to ensure compatibility of gear, communications equipment, communication details for quick reaction forces and emergency

medical services, routes, objectives, and mission understanding. Supporting partners, such as Joint Terminal Attack Controllers, Explosive Ordnance Disposal teams, or K-9 Handlers, are encouraged to participate in mission planning and support CTO activities. When AFOSI agents are teamed with a Security Forces Tactical Security Element (TSE), Battle Drills should be conducted before every mission.

Chapter 2

JOINT AND NATIONAL INTELLIGENCE ORGANIZATIONS, RESPONSIBILITIES, AND PROCEDURES

2.1. Organization. AFOSI prepares and organizes combat-ready forces to meet the needs of the Department of the Air Force. This implies a high level of training, flexibility in organization and equipment, and professional leadership. Although a standard force structure is not realistic for all contingencies, a deployed AFOSI force should have the following elements to effectively conduct CISFP in concert with joint or combined command goals and objectives.

2.1.1. Leadership. Deployed AFOSI expeditionary leaders, detachment commanders or special agents-in-charge, report directly to the designated agent who is part of, or coordinates closely with, the Commander of Air Force Forces staff.

2.1.2. Special Agents. AFOSI special agents should be trained in the CI collection activities listed in **paragraph 1.2**, the competencies listed in **Attachment 2**, and in the CTO Execution Cycle during the requisite pre-deployment training prior to conducting CISFP activities in an expeditionary environment.

2.1.3. Administrative Support. Deployed administrative personnel generally have the requisite training and security clearances to conduct support functions (e.g., office management, human resources, executive support, postal/official mail, commander programs, and limited client level information technology support) that enable the AFOSI unit or personnel to conduct the CISFP mission.

2.1.4. TSE. Threat dependent, AFOSI units and personnel should conduct CISFP with dedicated TSE in contested, complex, hostile and uncertain environments. A TSE provides the manpower, equipment, and firepower to enhance freedom of movement beyond the established base perimeter, independently of other ground maneuver units.

2.1.5. Analysts. AFOSI units should have embedded analysts with the requisite skill and training to analyze adversary threats. AFOSI embedded analysts should continuously gather and fuse relevant threat information from a broad array of sources. CI analysis helps focus collection and targeting activities.

2.1.6. Linguists. AFOSI units should have embedded linguists, specializing in native language, dialects, and cultural nuances, in the operational environment. The linguists should be vetted and have appropriate security clearances.

2.1.7. Intelligence Community integration/imbeds. AFOSI units should have organic IC capability within units conducting CISFP mission. These capabilities help provide force protection and expand other operational competencies.

2.2. Command Relationships. AFOSI supports combatant command theater campaign plans throughout the range of military operations, such as security cooperation, crisis response, and large-scale combat operations. Therefore, command relationships with supported commands vary across this spectrum. AFOSI Commanders direct the activities of those forces assigned or attached to an AFOSI unit. Command relationships in a joint environment for AFOSI operations are described in Joint Publication (JP) 1, Doctrine for the Armed Forces of the United States; JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations; and JP 3-10, Joint

Security Operations in Theater. When supporting a Secretary of Defense-approved operation, command authority for AFOSI forces conducting CISFP is delegated from the Joint Force Commander (JFC), through the COMAFFOR, to the designated senior deployed agent. Administrative control (ADCON) for AFOSI forces remains within the AFOSI chain of command at all times.

2.2.1. The COMAFFOR exercises operational control (OPCON) over AFOSI CISFP activities. The Secretary of the Air Force retains responsibility for law enforcement, CI investigations, and associated matters, and exercises this responsibility through the Commander, AFOSI. In the case of forces attached to another Service, responsive to a validated Request for Forces (RFF), OPCON may be delegated to the commander holding OPCON over all RFF forces.

2.2.2. AFOSI personnel not attached to an Air Expeditionary Task Force, who are performing the CISFP mission in a Joint Operational Area (JOA), are normally under the ADCON of the AFOSI senior deployed agent in theatre (e.g., personnel providing support to a contingency response group/contingency response element).

2.2.3. AFOSI routinely requires additional support elements to effectively conduct CISFP in concert with Service or joint command goals and objectives. When AFOSI requires Department of the Air Force forces to provide additional support elements, support requirements should be defined in a component's Operations Order (OPORD), support plan, or similar issuance, as appropriate for the location and area of operations. When TSE is part of the CTO package, AFOSI is the primary customer and will receive priority in mission planning. Conflicts between AFOSI and TSE may occur depending on theater dynamics, and the type of support required to achieve service or joint command objectives. It is imperative that AFOSI and TSE leaders resolve any such conflicts expeditiously at the lowest level possible, due to a high possibility of degraded or unavailable reach back communications in environments where disagreements may manifest.

2.2.4. AFOSI detachment commanders or special agents-in-charge normally coordinate their unit's CTO activities in hostile, highly contested, and uncertain environments with the appropriate base operations center (e.g., Base Defense Operations Center [BDOC], Tactical Operations Center [TOC], Battle Space Owner, etc.) and maintain communications with that element to facilitate freedom of movement, unity of effort, and safety of forces. AFOSI personnel, when operating in a joint/combined environment, must understand the rules of engagement (ROE), or the Rules for the Use of Force (RUF), established by the joint force commander. AFOSI personnel should also establish Standard Operating Procedures for situations of degraded or unavailable communications.

Chapter 3

CTO EXECUTION CYCLE

3.1. The CTO Execution Cycle. CISFP contributes to a keen awareness of the operating environment including Intelligence Preparation of the Operational Environment, and it incorporates the full range of functions/activities AFOSI uses to find, fix, track, neutralize, and assess the adversary. CTO activities help create a sustained permissive environment for air, space, and cyberspace operations. CTO capabilities are widely variable depending on their application combined with the prevailing threat, threat state, environment, friendly forces available, ROE, RUF, applicable laws, and other factors that characterize an operational area.

3.2. The five phases of the CTO Execution Cycle: Find, fix, track, neutralize, and assess (see **Figure 3.1**).

3.2.1. Find. The find phase requires clearly designated guidance. This guidance is typically provided via established priority intelligence requirements and associated collection requirements. These requirements drive CI collection planning and operations. CI collections lead to the detection of current and emerging targets. Tailored all-source analysis drives and focuses CI collections activities. AFOSI personnel should be familiar with the multiple targeting cycles present in a joint/combined operating environment and can be attached to support operational elements/capabilities in a limited fashion when skill sets specific to AFOSI (site exploitation, field interviews, tactical questioning, and MCC) are requested and approved with agent safety as the first priority.

3.2.2. Fix. The fix phase uses analysis and prioritization to determine if an emerging target is worthy of engagement. It may begin when an emerging target is detected or soon thereafter. When an emerging target is detected, sensors (human source networks, intelligence, surveillance, and reconnaissance (ISR) platforms), liaison activities, specialist activities, and information operations are focused to confirm the target's identity and precise location. Target location and other information must be accurately refined to permit tracking and neutralization. The completion of the fix phase results in a confirmed target with a designated CTO named operation.

3.2.3. Track. Tracking is done with the initiation/continuation of specific and directed CI collection and investigative activities. Tracking is also accomplished with the employment of specific ISR platforms. Information obtained during this phase is compiled and documented in a comprehensive target package.

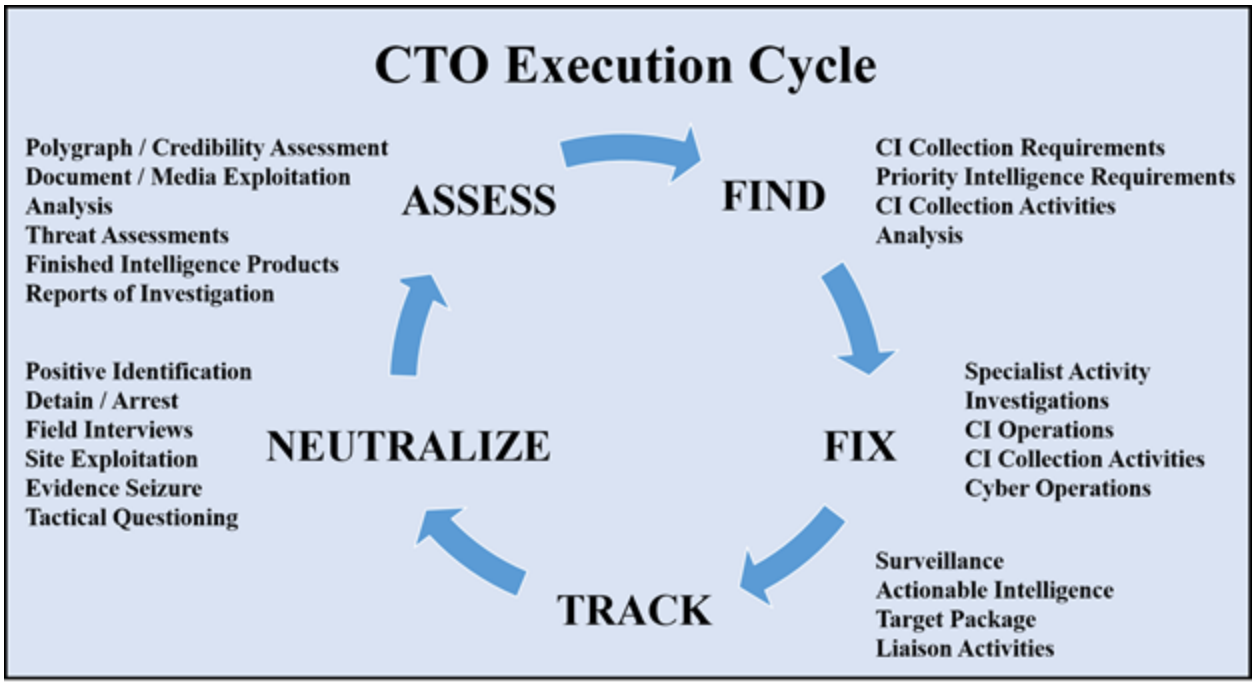
3.2.4. Neutralize. The neutralize phase begins after collected information is determined to be credible. Actionable intelligence or a comprehensive target package may be provided to a direct action authority for neutralization of the threat. AFOSI activities in this phase may include: positive identification; surveillance (physical, technical, or both); apprehension; recruitment; influence operations; and computer network exploitation. AFOSI forces disseminate actionable intelligence to direct action units and operations centers to support exploitation, seizure, SE, cordon and search, detention, or capture/kill operations.

3.2.4.1. Careful consideration of the intelligence gain-loss (IGL) balance must be made. It may be appropriate to delay engagement to allow better intelligence gathering and validation of veracity on a network of threats rather than take action on a single target.

3.2.4.2. In hostile and uncertain environments, AFOSI normally coordinates with maneuver units within the battlespace for target package execution. Following the execution of a CTO target package, AFOSI special agents may participate in field interviews, tactical questioning, and SE, including documenting the site, searching the site, prioritizing exfiltration, seizing evidence, and exploiting materials.

3.2.5. Assess. Tactical assessments determine the effectiveness of executed CTO activities. The principal question answered during the assess phase is whether desired effects and objectives were achieved. In cases of fleeting targets, quick assessments from trusted sources may be required in order to make expeditious re-attack recommendations.

Figure 3.1. The CTO Execution Cycle.



3.3. Reporting.

3.3.1. CTO reports contribute to commanders' overall awareness of the OE. AFOSI reports normally are disseminated to the intelligence and law enforcement communities, as appropriate, at all levels and during all phases of the CTO execution cycle. These reports include, but are not limited to, suspicious incident reports, intelligence information reports (IIRs), comprehensive target packages, analytical products, and spot reports. In certain situations, AFOSI reports the results of activities, such as field interviews and SE, including biometric evidence from accredited laboratory reports, to host-nation counterparts for inclusion into prosecution processes. After proper exploitation, AFOSI can provide material evidence collected during SE directly to host nation prosecutors and law enforcement agencies for their use.

TERRY L. BULLARD, Brig Gen, USAF
Commander
Air Force Office of Special Investigations

Attachment 1

GLOSSARY OF REFERENCES AND SUUPPORTING INFORMATION

References

AFI 10-403_AFOSISUP, *Deployment Planning & Execution,* 23 July 2019

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

AFMD 39, *Office of Special Investigations,* 14 April 2020

AFOSII 71-144, Volume 1, *Execution of AFOSI's Counterintelligence Mission*, 1 May 2019

JP 1, *Doctrine for the Armed Forces of the United States,* 23 Mar 2013 (as Amended through 12 July 2017)

JP 1-02**,** *DoD Dictionary of Military and Associated Terms*, as of June 2020

JP 1-04, *Legal Support to Military Operations*, 2 August 2016

JP 2-01, *Joint and National Intelligence Support to Military Operations*, 5 July 2017

JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations,* 6 April 2016

JP 3-0, *Joint Operations*, 17 January 2017 (as Amended through 22 October 2018)

JP 3-01, *Countering Air and Missile Threats*, 21 April 2017

JP 3-05, *Special Operations*, 16 July 2014

JP 3-10, *Joint Security Operations in Theater,* 25 July 2019

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ADCON—Administrative Control

AFOSI—Air Force Office of Special Investigations

BDOC—Base Defense Operations Center

CI—Counterintelligence

CISFP—Counterintelligence Support to Force Protection

COMAFFOR—Commander of Air Force Forces

CTO—Counterthreat Operations

DAF—Department of the Air Force

DOD—Department of Defense

IC—Intelligence Community

ID—Integrated Defense

IGL—Intelligence Gain-Loss

IIR—Intelligence Information Report

ISR—Intelligence, Surveillance, and Reconnaissance

JFC—Joint Forces Commander

JOA—Joint Operational Area

JP—Joint Publication

MCC—Military CI Collections

OE—Operational Environment

OPCON—Operational Control

OPORD—Operations Order

RFF—Request for Forces

ROE—Rules of Engagement

RUF—Rules for the Use of Force

SE—Site Exploitation

TACON—Tactical Control

TOC—Tactical Operations Center

TSE—Tactical Security Element

TTP—Tactics, Techniques, and Procedures

Terms

Administrative Control (ADCON)—Direction or exercise of authority over subordinate or other organizations in respect to administration and support.

Counterintelligence (CI)—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

Counter Surveillance—All measures, active or passive, taken to counteract hostile surveillance.

Direct Action (DA)—Short-duration strikes and other small-scale offensive actions conducted as a special operation in hostile, denied, or diplomatically sensitive environments and which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets.

Hostile Environment—Operational environment in which hostile forces have control, as well as the intent and capability, to effectively oppose or react to the operations that a unit intends to conduct.

Liaison—That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action.

Neutralize—1. As pertains to military operations, to render ineffective or unusable. 2. To render enemy personnel or materiel incapable of interfering with a particular operation. 3. To render safe mines, bombs, missiles, and booby traps. 4. To make harmless anything contaminated with a chemical agent.

Operational Control (OPCON)—The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission.

Permissive Environment—Operational environment in which host country military and law enforcement agencies have control as well as the intent and capability to assist operations that a unit intends to conduct.

Positive Identification—An identification derived from observation and analysis of target characteristics including visual recognition, electronic support systems, non-cooperative target recognition techniques, identification friend or foe systems, or other physics-based identification techniques.

Protective Service Operations (PSO)—The use of specialized techniques and procedures by trained personnel to ensure a principal's personal safety and security during a specific event, while traveling, or over an extended period of time. When required, a PSO can be tailored to provide 24-hour protection.

Rules Of Engagement (ROE)—Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered.

Site Exploitation (SE)—A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations.

Surveillance—The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

Tactical Questioning—Direct questioning by any DoD personnel of a captured or detained person to obtain time-sensitive tactical intelligence at or near the point of capture or detention and consistent with applicable law.

Target Packages—Targeting information provided by AFOSI to direct action units/authorities (Army, SOF, Coalition Forces, Host Nation Police etc.) for the purposes of identifying and neutralizing threats.

Technical Services—This support encompasses two distinct mission sets: the DAF's Technical Surveillance Countermeasures (TSCM) Program and AFOSI's technical surveillance program. AFOSI is responsible for executing DAF's TSCM Program, which includes techniques and measures to detect, neutralize, and/or exploit a wide variety of foreign technical surveillance technologies that are used to obtain unauthorized access to classified and sensitive information. AFOSI also provides technical surveillance support, including covert video and audio surveillance, vehicle tracking, photo surveillance, lock bypass, wiretap and other esoteric surveillance techniques.

Uncertain Environment—Operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended operational area.

Attachment 2

SKILLS LIST

Table A2.1. Skills List.

Advanced Firearms & Tactics	Recognize & Neutralize Improvised Explosive Devices
Deployed Concept of Operations	Self-Defensive Tactics
Deployed Liaison	Small Unit Tactics
Deployed Stress Management	Survival, Evasion, Resistance & Escape
Deployed Theatre & Cultural Orientation	Tactical Combat Casualty Care
Developing Standard Operating Procedures	Tactical Communications
Global Positioning System Use	Tactical Foot Movements
High Value Target Packages	Tactical Questioning / Interviews
Individual & Field Equipment Use	Tactical Vehicle Movements
Intelligence Information Report Writing	Terrorism / Insurgency TTPs
Land Navigation Map & Compass	Threat Detection / Attack Recognition
Military CI Collections Operations	Urban Operations
Night Operations	Vehicle Search & Security
Night Vision Techniques & Procedures	Working with Linguists
Operational Planning	Working with Ground Maneuver Units
Personal Security Operations	
Note: The following list contains examples of skills on which AFOSI agents should be trained prior to conducting CTO.	

Attachment 3

READING LIST

Figure A3.1. Recommended Reading List.

AFI 16-402, *Counter-Insider Threat Program Management,* 17 June 2020
AFOSI Manual 71-114, *Surveillance Operations,* 30 June 2009
AFOSI Manual 71-144 V1, *Execution of AFOSI's Counterintelligence Mission*, 1 May 2019
AFOSI Manual 71-144 V3, *Protective Services Operations, 29 September 2020*
AFPD 31-1, *Integrated Defense*, 21 June 2018
AFTTP 3-4.7, *Contingency Response*, 30 September 2017
Army Field Manual 3-24, *Insurgencies and Countering Insurgencies,* 13 May 2014
DHE-M Vol. I 3301.001 (S//NF), *Collection Requirements, Reporting, and Evaluation Procedures* (U), Incorporating Change 2, 1 Feb 12
DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 27 April 2018
DoDD 5240.02, *Counterintelligence*, 16 May 2018
DoDD 5240.06, *Counterintelligence Awareness and Reporting,* 31 August 2020
DoDI 5240.04, *Counterintelligence Investigations,* 18 September 2020
DoDI 5240.05, *Technical Surveillance Countermeasures*, 27 August 2020
DoDI S-5240.09, *(U) Offensive Counterintelligence Operations*, 18 July 2016
DoDI S-5240.17, *(U) Counterintelligence Collection Activities*, 14 March 2014
DoDI 5240.22, *Counterintelligence Support to Force Protection*, 8 September 2020
DoDI 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat*, 30 April 2018
JP 1, *Doctrine for the Armed Forces of the United States,* 31 May 2016
JP 1-02**,** *DoD Dictionary of Military and Associated Terms*, as of June 2020
JP 2-01, *Joint and National Intelligence Support to Military Operations*, 5 July 2017
JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*, 6 April 2016
JP 3-0, *Joint Operations*, 17 January 2017 (as Amended through 22 October 2018)
JP 3-07.2, *Antiterrorism,* 14 March 2014
JP 3-10, *Joint Security Operations in Theater,* 25 July 2019