ARMY
ANTITERRORISM OFFICER
READY REFERENCE

VIGILANCE

U.S.ARMY Army Strong℠

Always Ready, Always Alert
Because someone is depending on you

CONTENTS

INTRODUCTION

Purpose

The purpose of this booklet is to provide a **"ready reference" for Army Antiterrorism Officers (ATO)**. The information contained within this booklet includes general information on the terrorist threat, how to maintain antiterrorism (AT) awareness, an overview of Army suspicious activity reporting programs and systems (such as iWATCH Army, iSALUTE, and eGuardian), and an overview of key AT program elements which provide guidance and tools for ATOs for the execution of their command specific plans and programs. By understanding the terrorist threat and the resources and tools available to guide and assist ATOs, the Army community can sustain a reasonable level of vigilance which will reduce the risk of becoming a terrorist target and contribute to the overall protection of Army communities.

Overview

Terrorism is an enduring, persistent, worldwide threat to our Nation and our Army communities at home and abroad. Extremist ideologies and separatist movements

continue to have an anti-western and anti-U.S. orientation which threatens our Nation. Porous international borders and unimpeded access to social media presents increased opportunity for terrorists and their affiliates to travel and use the internet to provoke religious ideologies and radicalization at an increasing scale. Army communities must be capable of deterring, preventing, and defending against the full range of terrorist tactics.

The Terrorist Threat

A *terrorist* is an individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives (JP 3-07.2). History points to acts of terrorism taking place roughly 2,000 years ago. In the late 20th and early 21st centuries, international terrorist actions and groups continued to grow, along with affiliate groups and persons who mimic terrorist tactics. The attacks of 11 September 2001 and the 2008 Mumbai attacks, illustrate the **possibility of unpredictable asymmetric tactics**. Increasing the level of complexity and sphere of influence is terrorists' ability to encourage citizens living within U.S. borders to execute attacks on behalf of their cause. Given the long history of terrorist attacks and the

adaptive nature of the threat, awareness of the threat methodology and tactics is a first line of defense.

TERRORIST METHODOLOGY AND TACTICS

How Terrorists Select Targets

Terrorists' target selection process considers three elements—location, association, and opportunity—and generally follows a deliberate planning cycle regardless of the intended target and amount of time available to prepare for an operation.

» **Location:** Terrorists may target **locations frequented by Americans** (such as military installations or facilities, or certain hotels, apartment buildings, public transportation centers, and nightclubs frequented by Americans). Individuals should maintain heightened awareness in these locations and leave immediately if they observe suspicious behavior or activity.

» **Association:** Terrorists may focus pre-operational surveillance or attacks on obvious American tourists or personnel associated with the U.S. military. When possible, avoid disclosing your U.S.

affiliation. When overseas, try to blend in with the local populace.

» **Opportunity: Terrorists look for "soft targets."** A soft target is a person, information, or facility in which the terrorist perceives they have good chance of a successful attack and a low risk of interference by law enforcement or security forces. To reduce opportunity, individuals should maintain vigilance, practice good personal security habits, and alert the proper authorities of observed suspicious behavior.

Terrorist Planning Cycle

The figure above depicts the terrorist planning cycle as viewed by most U.S. intelligence agencies. The blocks generally represent the amount of overall time dedicated to accomplishing the specified task. The terrorists' planning, preparation, and execution cycle may take place over many months or even years for a single, specific target. Note that the **longest period is dedicated to intelligence and surveillance** activities. Because terrorist personnel must expose themselves to effectively perform intelligence and surveillance activities, they are most vulnerable to detection by an alert and attentive Army community and by civilian law enforcement and security personnel.

Initial intelligence and surveillance may be accomplished using multiple methods (such as open-source information, internet accessed imagery, ground surveillance, etc.). The initial surveillance conducted by terrorist group members to gather information on a broad

range of targets will often be conducted by less qualified and possibly "expendable" group members or by associates or affiliates of the main terrorist organization.

Surveillance operations may include tests of security to determine security force response to unknown threats. The final, pre-attack surveillance may be reserved for a separate cell to maintain operations security (OPSEC) or assigned to more seasoned professionally trained intelligence experts. The final surveillance may be conducted by the actual terrorists who will execute the operation.

Advanced terrorist groups operate within extremely compartmentalized specialties for OPSEC reasons. Often those who conduct the initial surveillance do not know those who conduct the final surveillance, and none of the surveillance personnel may know who will execute the attack. Other members of the group (planners, support, financiers, etc.) are often compartmentalized and have nothing to do with the intelligence gathering, surveillance activities, or the attack.

Terrorist Tendencies

- Rotate surveillance personnel to avoid detection
- Abort the mission if surveillance, rehearsals, or pre-attack tasks are observed
- Use rented property or isolated locations as safe havens to avoid detection
- Conduct rehearsals and practice runs to refine operational skills
- Exploit social media in an attempt to influence or recruit supporters
- Test security on the actual target prior to the attack
- Postpone or cancel the operation because of random changes in security posture
- Seek standoff from anticipated response forces unless willing to die for the cause

ACTIVE SHOOTER THREAT

An active shooter is defined as an **armed person who uses deadly force** on other persons and continues to do so while having unrestricted access to additional victims (Source: U.S. Army Military Police School, Active Shooter Program of Instruction). The event that began this new age of threat tactics was the Texas Tower Sniper (1 August 1966) in which the gunman established a high ground advantage overlooking his target area which substantially hampered an effective police response. More recent assaults—beginning with the North Hollywood shootout (28 February 1997), Columbine massacre (20 April 1999), Virginia Tech shooting (16 April 2007), Mumbai terrorist attacks (26-29 November 2008), and Fort Hood shooting (5 November 2009)—involved an array of active shooter tactics.

An active shooter may be a **current or former employee** associated with the U.S. Army (Soldier, Department of Army Civilian, contractor, or family member). An active shooter could also be an **individual not directly associated with the Army who gains unrestricted access** to an installation, standalone facility, or unit area.

Individuals who evolve into active shooters often exhibit signs of high risk behavior or an escalation of violence leading up to the shooting. As such, **recognizing the indicators of violent behavior may include** one or more of the following (not all inclusive):

- Increased use of alcohol or drugs
- Unexplained increase in absenteeism or vague physical complaints
- Depression or withdrawal
- Increased severe mood swings and noticeably unstable or emotional responses
- Increasingly talks about personal problems or problems at home
- Increase in unsolicited comments about violence and weapons

How to Respond During an Active Shooter Situation

When Shooting Begins	When the Police Arrive
Evacuate • Have an exit route and plan in mind • Leave your belongings behind • Keep your hands visible **Hide Out** • Hide in an area out of the Active Shooter's view • Lock doors and block entry to your hiding place **Take Action** • As a last resort • Only when your life is in imminent danger • Attempt to incapacitate the Active Shooter	• Try to remain calm • Obey all Police instructions • Put down any items in your hands (such as backpacks, phones, jackets) • Raise your hands, spread your fingers, and keep hands visible to Police at all times • Avoid quick or sudden movements • Avoid pointing, screaming, or yelling • Do not stop to ask officers for help or direction while evacuating

FUNDAMENTALS OF ANTITERRORISM AWARENESS

General Awareness Tips

Maintain situational awareness of your surroundings at all times. Pay particular attention to activity happening around you in order to identify anything unusual. If necessary, leave the area and report suspicious activity or behavior to local authorities. **Trust your instincts!**

Protect your personal information. Do not reveal details of your personal life (such as where you live, work, family members, your association with the U.S. military, email address or phone numbers) to anyone you don't know and trust.

Do not discuss personal information or military missions in public, on the telephone,

or on the internet. Take extra precaution with **social media networks (such as *Facebook*, *Twitter*, and blogs)—avoid posting or providing personal information. CAUTION:** Pictures uploaded from mobile phones often have geo-tracking data embedded within the file which can reveal the specific location or address. Criminals and terrorists are known to use these forums for open source information gathering and recruitment and these media do not provide "secure" communications.

Awareness at Home

Basic security begins with the home**. Make sure door and window locks and exterior lighting function properly.** Children should keep doors and windows locked when home alone.

Participate in a **neighborhood watch program** to establish a shared responsibility for the safety and security of your local community.

Be prepared for an emergency that may require your family to "shelter-in place" or relocate with little advanced notice. Make a **family emergency plan** and ensure all family members understand what to do in each of these scenarios.

Awareness at Work

Know the emergency evacuation procedures for your workplace.

Know the bomb threat procedures and how to report threats.

Understand what to do in an "active shooter" threat scenario.

Awareness while Travelling

Maintain a "low profile" when travelling abroad. Try to blend in with the local populace through your dress and appearance. Know the location of safe havens and carry with you the local emergency telephone numbers.

Understand the culture where you are traveling and learn basic survival phrases (such as "I need a police officer" and "I need a doctor"). Avoid civil disturbances or demonstrations of any kind—these events can turn violent with little to no advanced warning.

Public venues with large crowds present lucrative terrorist targets. Understand the **risks of attending public venues** based on the history of terrorist attacks in your area and security provided at the event.

Never travel alone; always travel in groups of two or more. Think ahead and choose safe travel modes and routes.

Awareness for Army Families

Talk to your family about the potential for terrorist acts to impact your family. None of us are immune, and acknowledging that fact is the first step to a **proactive security mindset**. The level of risk to each family varies depending on factors such as existence of terrorist groups and their intentions; locations where you live, work, and travel; and the vulnerability associated with your personal security habits. AT officers through support to Family Readiness Groups can help military parents understand how to assess risk adopt effective personal protection measures. Below are some of the fundamentals of security that can enhance the overall safety of family members.

Parents

Maintain awareness of what is happening around you. **Be prepared for the unexpected**, and know what to do if you feel threatened in any way.

Protect your personal information at all times. **Do not discuss personal information or military missions in public, on the telephone or internet** (such as email, blogs, *Facebook*).

Report suspicious behavior or activity to local law enforcement authorities.

Young Children

Pre-teen age children are generally too young to understand the concept of "terrorism" and why terrorists attack the innocent. However, it's not too early for parents to discuss the concept of "Stranger Danger" which is covered well in books, stories, and information available to the public on the internet. This approach offers a useful method to begin introducing young children to the concept of suspicious behavior and the need to tell a trusted person when they feel they may be in danger.

The National Crime Prevention Council's online site "McGruff.org" (http://www.mcgruff.org/) offers useful information and ideas on how parents can talk about dangers with their young children.

Parents are encouraged to talk to their children about the dangers they may face and teach them how to react. If children **see something** unusual they should **say something** (tell a parent, a relative, or a teacher).

By the time children grow into their early teenage years, most are exposed through media to the effects of terrorist attacks. As such, teenagers are more prepared for family discussions focused directly on terrorism and more likely to be receptive to parental guidance on personal protective measures.

Teenagers

As teenagers enjoy increased personal freedoms their risk of personal safety and security also increase. Some of these risks include criminal and terrorist related activities.

Social network sites (such as *Facebook*, *Twitter*, and blogs) present a unique set of challenges and risks for teenagers. Teenagers should be aware of the risks associated with these sites (such as identity theft, criminal or terrorist group recruitment, seeking information to target the military). **Revealing personal data can lead to criminal exploitation as well as recruitment or influence by radical or extremist ideological groups.**

Basic security measures for teenagers include: never travel alone, carry a cell phone which includes local emergency contact numbers for the police, know safe haven locations (such as police, hospital), and keep parents informed of where they are going and when they will arrive and return.

Parents should know who their teenagers associate and communicate with during normal daily activities as well as on social networking sites and the internet.

Suspicious Activity

Indicators of potential terrorist activities should be reported to Military Police or law enforcement officials immediately. **Examples of suspicious activities** include:

- People drawing or measuring important buildings
- People asking questions about security forces, security measures, or sensitive information
- Briefcase, backpack, suitcase, or package left unattended
- Vehicle parked in NO PARKING ZONES near important buildings/facilities
- People in restricted areas where they are not supposed to be
- A person wearing clothes that are too big and too hot for the weather
- Chemical smells or fumes that worry you
- People purchasing supplies or equipment that can be used to make bombs
- People purchasing weapons or uniforms without proper credentials

Suspicious Activity Reporting Methods	What to Report
• Military Police • Local law enforcement • Security forces • Chain of command • Parents (for children)	• Day and time activity occurred • Where activity occurred • How many people were involved • Number and type of vehicles • What type of activity • Describe what you saw or heard • Provide pictures if you took any

Indicators of Terrorist Associated Insider Threat

This focus area includes identifying indicators of violence and radicalization to ensure law enforcement and unit leaders have the information and tools needed to identify and respond to internal threats.

The following behavior may be *indicators of potential terrorist activity or insider threat* and should be reported immediately to the local counterintelligence office, Military Police, law enforcement, or unit leadership:

- Advocating violence, the threat of violence, or use of force
- Advocating support for international terrorist organizations or objectives
- Providing financial or other material support to a terrorist organization
- Association with or connections to known or suspected terrorist
- Repeated expression of hatred and intolerance of American society
- Repeated browsing or visiting internet websites that promote or advocate violence

- Expressing an obligation to engage in violence in support of terrorism
- Purchasing bomb making materials
- Obtaining information about the construction of explosive devices
- Active attempts to encourage others to violate laws/orders or disrupt military activities
- Family ties to known or suspected terrorist or terrorist supporters

SUSPICIOUS ACTIVITY REPORTING PROGRAMS

iWATCH Army

iWATCH Army is an AT awareness program focused on terrorist activity and seeks to educate the Army community on the indicators of potential terrorist activity and *encourage citizens to report suspicious activity* to military police or law enforcement for investigation.

Trust Your Instincts: Individuals rely on their senses every day of their lives. If a behavior or activity makes you feel uncomfortable, **Report It!**

What to Report: give as many details as possible—here is a checklist:

- The date and time?

- Where it happened?
- What you witnessed?
- A description of who was involved:
    * Male or female?
    * How tall?
    * Build?
    * Hair color, skin color, age?
    * English speaking or another language?
- Was there a car—did you note the license plate number?
- Have you seen this activity before?

Reports received by law enforcement are analyzed and, as appropriate, entered into eGuardian—the Department of Defense (DoD) suspicious activity reporting (SAR) system. Entry of suspicious activity data into eGuardian enables access to the data by other Federal law enforcement agencies through the Federal Bureau of Investigation's Guardian system.

iSALUTE

iSALUTE is an Army counterintelligence reporting program to **prevent espionage, sabotage, subversion, and international terrorism**. iSALUTE seeks Army-wide community support to report threat incidents, suspicious activity, and counterintelligence matters that are potential indicators of espionage, terrorist-associated insider threat, and extremist activity.

Suspicious Activity Reporting Programs

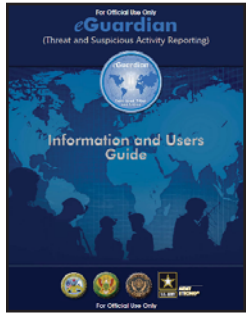
Threat awareness and education training is designed to ensure that the Army community recognizes and reports incidents and indicators of:

- Attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Army
- Indicators of potential terrorist-associated insider threats
- Illegal diversion of military technology or technology-based information

- Unauthorized intrusions into automated information systems
- Unauthorized disclosure of classified information
- Indicators of other incidents that may indicate foreign intelligence or international terrorism targeting the Army

Information Sharing. There will always be some overlap between iWATCH Army and iSALUTE programs. The key point for members of the Army community is **to understand the indicators of suspicious activity and REPORT suspicious behavior** to local law enforcement and/or counterintelligence for further investigation—when in doubt report! Law enforcement and counterintelligence agencies are responsible for sharing threat information, conducting detailed analysis, and reconciling information gaps.

eGuardian – Suspicious Activity Reporting System



The eGuardian system is a sensitive but unclassified reporting system operated by the Federal Bureau of Investigation (FBI) to **collect terrorist threat and suspicious activity information having a potential link to terrorism**. The data allows the FBI to share information with other Federal, State, local, and Tribal law enforcement.

In May 2010, the Secretary of Defense designated the eGuardian system as the authorized DoD law enforcement suspicious activity reporting (SAR) system.

eGuardian is **restricted to law enforcement personnel**, and is accessible through the FBI's Law Enforcement Online (LEO) Information System. eGuardian links unclassified, for official use only, and law enforcement sensitive reporting information to the FBI's Guardian program which is a classified FBI network designed to allow

for the transmission of terrorist threat and suspicious activity information.

The ***eGuardian Threat and Suspicious Activity Reporting Information and Users Guide*** provides Army law enforcement and criminal investigators detailed information on the system capabilities and functions. Included within the guide is the responsibility of key agencies, procedures for requesting access and obtaining training, user roles, information flow, and analytical process. An annex within the guide includes the **reportable categories of suspicious activity**.

LEADERS ROLE IN ANTITERRORISM

Army leaders, regardless of their roles, should ask themselves, **what can I do to enhance AT and awareness** for my unit or the Army community?

A sample of what leaders can do to promote AT awareness include:

- Understand the AT plans and program within your area of responsibility
- **Be an advocate for the AT program**
- Promote AT awareness throughout the Army community
- Conduct a risk assessment of the likelihood of terrorist activity for your area
- Ensure plans and measures are in-place to mitigate identified risks
- Understand the importance of information sharing—**"Who Else Needs to Know?"**

- Understand escalation of violence and how indicators of high risk behavior may prevent violence in the workplace ("Insider Threat")
- Understand the purpose of iWATCH Army, iSALUTE, and eGuardian and how they fit within your AT plan or program
- Get Family Readiness Groups involved—provide them AT awareness training and keep them informed about the changes in local threat and protective measures

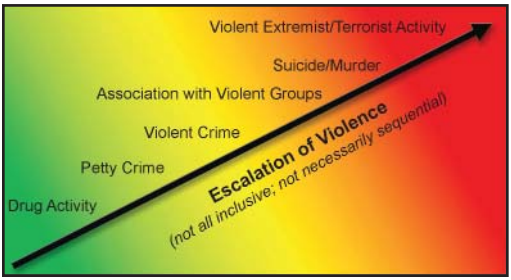
PREVENTING ESCALATION OF VIOLENCE

Preventing insider threats or terrorist attacks involves much more than physical security measures. **Recognizing the indicators of high-risk behavior** (such as criminal activity or associating with violent groups) **may prevent an escalation of violence**.

A sample of potential high risk behavior includes:

- Lack of positive identity within the community
- Participation in criminal activity
- Increased use of alcohol or drugs
- Diagnosed mental disorder or depression
- Increased severe mood swings or unstable emotional responses
- Increase in unsolicited comments about violent tendencies or weapons
- Defending extremist or radicalized views
- Unexplained selling or giving away of personal possessions

- Health based monitoring and treatment programs may include individuals with a greater risk of future violence



Escalation of Violence Spectrum

TENANT UNIT ANTITERRORISM RESPONSIBILITIES

Tenant Unit AT Responsibilities

Installation, garrison, and base commanders have overall responsibility for the security of personnel, information and infrastructure within their assigned geographical area of responsibility. Tenant units provide security for their own unit areas, forces, and critical assets, and provide individual or unit security augmentation as directed by the AT plan or in the case of emergencies, as directed by the host commander. To ensure effective AT plans, *tenant units must actively participate in the planning, execution, and incident response activities* to protect Army forces and assets from terrorist acts. As a minimum, tenant unit participation is required in support of the installation or garrison AT working group (ATWG) and the AT threat working group (TWG). Commanders of operational bases generally integrate the ATWG and TWG into their unit intelligence, operations, and planning processes.

AT Working Group (ATWG)

Installation and garrison commanders establish an ATWG that meets semi-annually, or more frequently depending upon the level of threat activity, to oversee the implementation of the AT program, to develop AT plans, and to address emergent or emergency AT issues. **Tenant unit participation ensures the AT plan accurately reflects the combined capabilities and resources of tenants** while at the same time ensuring tenants understand and are prepared to execute their assigned tasks. The installation or base AT plan should contain detailed instructions for tenant unit roles and responsibilities.

Threat Working Group

The TWG is organized and meets quarterly or more frequently, depending upon the level of threat activity, to develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries. **Tenant unit participation ensures all units on the installation or base maintain situational awareness of the terrorist threat** and processes are in place to rapidly disseminate imminent threat warning.

AT Exercises

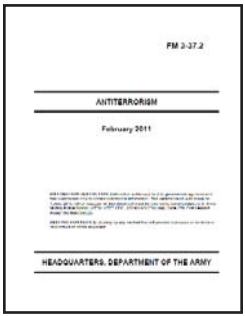
A full-scale exercise is the most complex of AT exercises. For key organizations and tenant units, a full-scale AT exercise activates all parts of the installation, garrison or base AT plan. The exercise should test the ability to implement RAM as well as increased FPCON levels. Throughout the exercise, **tenant unit responsibilities should be executed** to ensure plans are understood and adequate unit resources are available.

Incident Response

Installation, garrison, or base AT plans should include detailed terrorist threat/incident response (TT/IR) **plans that integrate the full capability of tenant unit capabilities** to defend from and mitigate the effect of an imminent terrorist threat. All forces that support the TT/IR plan should be pre-designated, trained together, and prepared to perform individual and collective crisis management tasks under the control of the incident commander.

AT DOCTRINE/POLICIES/ RESOURCES

AT Doctrine (FM 3-37.2, Antiterrorism)


FM 3-37.2

ANTITERRORISM

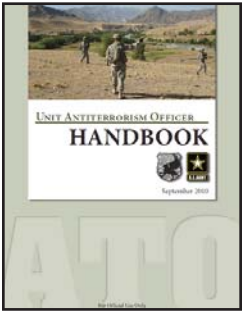
February 2011

HEADQUARTERS, DEPARTMENT OF THE ARMY

To address the growing and evolving threat of terrorism, the Army combined the most important elements of AT policy with the practical application and doctrinal wisdom gained from operational forces, installations, and standalone facilities. Sound doctrinal principles, tools, and processes have emerged by leveraging extensive AT expertise from across the force. **FM 3-37.2 now provides units with a blueprint to help build AT plans and programs. It outlines AT principles (assess, detect, defend, warn and recover)**, integrates AT within the combating terrorism framework and the protection warfighting function, and builds on the Army's effective operations and intelligence processes.

In addition to describing the characteristics of successful AT programs, the AT principles support the broader functional concept of protection. They provide operational forces with guidance about how to best protect personnel, units, information, operations, and critical assets from terrorist threats and attacks. Key protection measures include the integration of elements of other programs (physical security, information assurance, military and criminal intelligence, operations security, law enforcement, emergency management), persistent detection, shared understanding, and dissemination of threat information.

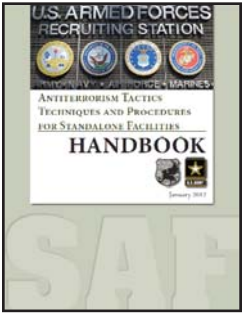
AT Officer Handbook



The *Unit ATO Handbook* is a technical publication focused on operating force unit ATOs at the brigade and battalion levels. Operating force units are defined as the forces the Army maintains for combatant commanders to use in contingencies. Operating units are organized under a modified table of organization and equipment. Army AT policy establishes the basic AT tasks and supporting standards that all Army organizations in the operating and generating forces are required to meet. The Unit ATO Handbook establishes a unit **AT framework for operating force ATOs to use in identifying and reducing terrorist threats to their unit operations, whether in garrison or a combat zone**. The handbook provides unit-level ATOs with detailed implementation guidance for the AT tasks and relevant unit standards in specific mission environments. It also provides detailed knowledge and procedures that will help ATOs

do their jobs more effectively. The handbook identifies specific actions and responsibilities that unit ATOs must perform to defend against terrorist tactics. The handbook will help unit ATOs integrate and synchronize AT requirements with other ongoing unit missions and activities. The handbook is **not intended to serve as a comprehensive single-source reference**. It is, however, intended to provide a reference for unit ATOs, covering their basic duties and responsibilities, augmented with specific tips, techniques, and hints to facilitate their assignment to a brigade or battalion staff.

Security for Standalone Facilities



The protection of Standalone Facilities (SAF) is a critical element of the Army's AT program focused on protecting personnel, information, and facilities against potential terrorist activities.

The methods to protect SAFs are considerably more complex than those measures taken to protect Army installations. **SAFs (such as recruiting stations and Reserve/Guard facilities) are embedded in civilian communities** and often do not have same level of protection as typically assigned to Army installations. Facilities that match this description are often referred to as potential "soft targets."

While some SAFs have barriers that define an operational area, most are an integral part of their environment and have no organic security or emergency response capabilities. As such, most are dependent upon the local community for security and threat information support.

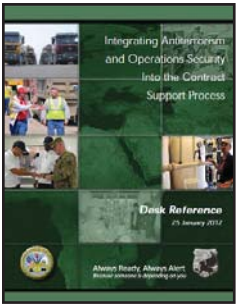
Protecting SAFs against a terrorist attack presents a particular challenge. Recent reports and actions indicate an **increased likelihood of attacks against SAFs from homegrown violent extremists and terrorists**. The terrorist threat has adapted to more vulnerable targets such as transportation systems, community gatherings, hotels, and facilities which present greater opportunities for successful attacks.

Because SAFs are embedded in the community and often represent an obvious visual image of the U.S. military, they may be the most likely terrorist target across the Army community.

The SAF Handbook provides to leaders of standalone facilities (SAFs) supplemental implementation guidance in executing AT responsibilities for their facilities and personnel.

"Antiterrorism Tactics, Techniques, and Procedures for Standalone Facilities," provides guidance to assist in building AT programs for these facilities. The handbook supplements AT policy and doctrine to help build viable defenses to prevent terrorist attacks. The handbook is available on the OPMG Army ATEP on AKO.

Integrating Antiterrorism and Operations Security (OPSEC) into the Contract Support Process



Recent attacks remind us that terrorists do not distinguish between combatants and noncombatants and may select targets specifically to effect military operations.

To achieve successful attacks, terrorists seek to exploit gaps in security—Army contract support services represent one such possibility.

Terrorists posing as contractors or exploiting a security gap in a contracted service could attack Army operations at unsuspected times and locations. Additionally, contractor employees may also become targets for terrorist attack.

Integrating Antiterrorism and Operations Security (OPSEC) into the Contract Support Process is a desk reference which includes tactics, techniques, and

procedures aimed at closing possible security gaps through increased focus on AT/OPSEC measures throughout the contract support process.

The Desk Reference offers suggestions for the performance work statement language and elements for a quality surveillance plan. It provides the necessary tools to ensure contracting specialists and AT/OPSEC officers work together to reduce the possibility of terrorist attacks related to commercially provided services on Army-controlled installations and facilities or during Army operations.

It also includes the requirement for an AT/OPSEC cover sheet as part of the process of submitting the contract requirements package.

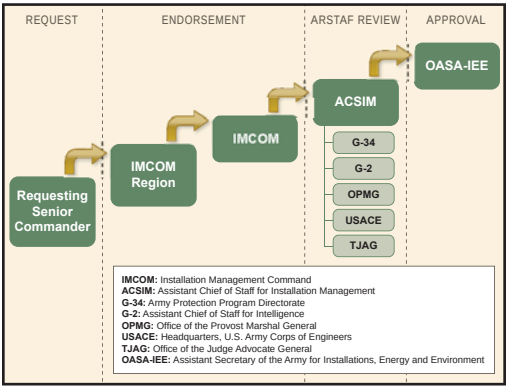
UFC Waivers/Exception Process

The Assistant Secretary of the Army for Installations, Energy and Environment ASA (IE&E) is **designated the approval authority for granting Army waivers and exceptions** to the requirements contained in the Unified Facilities Criteria (UFC) 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings" and UFC 4-010-02, "DoD Minimum Standoff Distances for Buildings."

Requests for waivers and exceptions will be made by responsible installation or activity commanders (or civilian equivalent position), endorsed by senior commanders and the chain of command (responsible ACOM, ASCC, DRU, or ARNG) and forwarded to the Assistant Chief of Staff for Installation Management (ACSIM) for headquarters Department of the Army (HQDA) coordination. Upon completion of HQDA coordination, ACSIM will prepare recommendation and forward the waiver requests to the ASA (IE&E) for final approval. Upon approval, installation and activity commanders will provide a copy of the waiver or exception to U.S. Army North.

All commanders seeking waivers or exceptions to requirements contained in UFC 4-010-01 and UFC 4-010-02 for any building or

portion of a building (permanent, temporary or expeditionary)—whether owned, leased, privatized, or otherwise occupied, managed or controlled by DoD—will **submit requests in accordance with the procedures established in HQDA ALARCT 254/2011, Unified Facilities Criteria Requirement Waivers and Exception Procedures, 121812Z JUL 11** (available on ATEP).



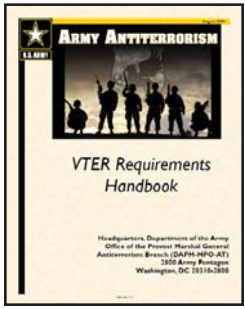
Army UFC Waiver/Exception Process

CONUS: the above process is applicable only in CONUS. USNORTHCOM Instruction 10-222 stipulates that DOD Components will continue to utilize their Service waiver process.

OCONUS: Geographic Combatant Commanders are the UFC waiver authority for their area of responsibility.

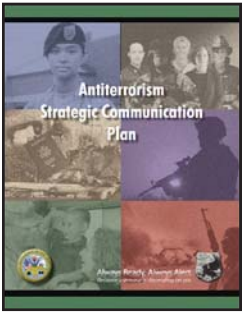
Note: Non-Installation Management Command installation or facility waiver requests are not endorsed by IMCOM but by their owning Army Command, Army Service Component Command, or Direct Reporting Unit and then routed to HQDA (Assistant Chief of Staff for Installation Management) for approval.

VTER Handbook



The VTER Requirements Handbook provides **information to assist ATOs in the development and submission of the command's Schedule 75 report**. Schedule 75 reports are specifically developed for submission of AT program requirements which the VTER MDEP supports. The handbook describes the process, timelines, detailed instructions, formats/examples, and requirements worksheets for AT requirement categories. The handbook assists ATOs in the development and submission of AT requirements which are validated as "critical" by the Installation Program Evaluation Group (II PEG).

AT Strategic Communication (SC) Plan (Desk Reference)



The AT SC Plan desk reference provides information explaining the Department of the Army strategy, policy, and implementation considerations to **incorporate AT awareness into command information programs**. Command specific AT SC Plans should serve as living documents for near-term and long-term planning as well as a guide for implementing a community wide AT awareness out-reach program. **Key elements of the AT SC Plan should include analysis of:**

- Target audience – conduct analysis to determine whom to communicate to
- Themes – understand the most important, relevant topics, and which audience(s) the topics relate to
- Messages – develop clear and concise messages to support the themes based on specific audience(s) needs

- Products – determine which products will communicate most effectively
- Communication venues – select the time and location to disseminate information
- Feedback – establish a mechanism to obtain feedback

AT Awareness Month Planning Guide

The purpose of this publication is to **provide Army leaders and AT officers with supplemental guidance for planning and preparing for observance of AT Awareness Month**. The primary objective of AT awareness month is to instill Army-wide heightened awareness and vigilance to prevent and protect people, information, and critical resources from acts of terrorism.

The guide includes information to assist ATOs in the planning and preparation phase and helpful hints on:

- how to leverage the command information program
- partnering with the public affairs office
- tips for advertising AT awareness month
- instruction on use of social media
- and sources for online references

ONLINE RESOURCES

OPMG Army ATEP on AKO

This is an Army Knowledge Online (AKO) website maintained by the Office of the Provost Marshal General. The site provides a wealth of AT products, tools, and resources for use by leaders and staff at all levels. **All of the products discussed and shown within this booklet are available online.**

(https://www.us.army.mil/suite/page/605757).

Army OneSource

Army One Source provides a link to AT awareness and iWATCH Army information through the iWATCH Army logo at the bottom of the Army OneSource homepage. Information on this site is easily accessible for Army families and others who do not have direct access to AKO.

(www.myarmyonesource.com)

Additional References

- **Army AT Policy (AR 525-13)** establishes the Army AT program to protect personnel, information, property, and facilities in all locations and situations against terrorism.
- **Antiterrorism awareness training** is available through the unit or installation AT officer. The training includes basic knowledge of the terrorist threat pertaining to air and ground travel; security at government facilities, hotels, and home; vehicle bomb threats; and hostage survival tips.
- **CJCS Guide 5260, Antiterrorism Personal Protection Guide: A Self Help Guide to Antiterrorism.** This guide offers useful information about terrorist threat awareness and personal protection measures.
- **PC 5260, Antiterrorism Individual Protective Measures.** This wallet card is a great reference tool to remind family members of basic security measures.

BE VIGILANT

Remain alert to changing conditions and suspicious activities

ANTICIPATE

Anticipate threats and make choices that reduce risk

DON'T BE A TARGET

Be anonymous and unpredictable

RESPOND & REPORT

Be responsive to security and law enforcement personnel; report suspicious or threatening activities



Always Ready, Always Alert
Because someone is depending on you