



ANG Total Force Awareness Training (TFAT)

Ancillary Refresher Program

Force Protection







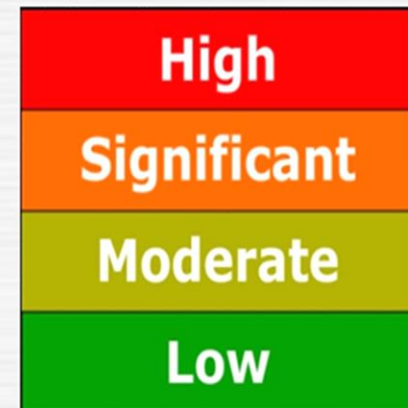
Terrorism Threat Levels

HIGH – Anti-U.S. terrorists are operationally active and use large casualty producing attacks as their preferred method of operation.

SIGNIFICANT – Anti-U.S. terrorists are present and attack personnel as their preferred method of operation.

MODERATE – Terrorists are present but there are no indications of Anti-U.S. activity.

LOW – No group is detected or the group's activity is non-threatening.





First factor

***Are there any
terrorist groups in
my area?***





Second factor



Are they violent?



If violent-

***Do they attack
Americans?***





Activity factor

***How active are
they?***





Sophistication factor



***How
sophisticated
are they?***





Cultural factors

***Will the local
population warn
Americans?***





Tactical factors

What tactics?
What type of
attack?





Operational factors

How do they operate?

Are they predictable?





Select and Identify Targets





Indicators of Potential Terrorist Activity

What to look for?



Surveillance

Someone recording or monitoring activities

Cameras

Note taking

Drawing diagrams

Writing on maps

Using binoculars





Elicitation

Attempts to gain information about military operations through various means.

Mail

Fax

Phone

In person





Test of Security



Attempts to measure reaction times by security forces or law enforcement.



Attempts to penetrate physical security barriers or procedures.



Acquiring Supplies

Purchasing or stealing materials such as:

Explosives

Weapons

Ammo

Uniforms

Flight Manuals

Passes or Badges

Any other controlled item





Dry Run

May include pre-operational surveillance, such as:

Mapping out routes

Determining traffic flow



Similar to a dress rehearsal/scrimmage





Deploying Assets

Placing people/supplies in position

Final opportunity to alert authorities.

See Something,
Say Something





AF Eagle Eyes



Neighborhood watch, on base and off.



Individual Protective Measures

General Security

Travel Security

In-Transit Security

Home Security

Cyber Security



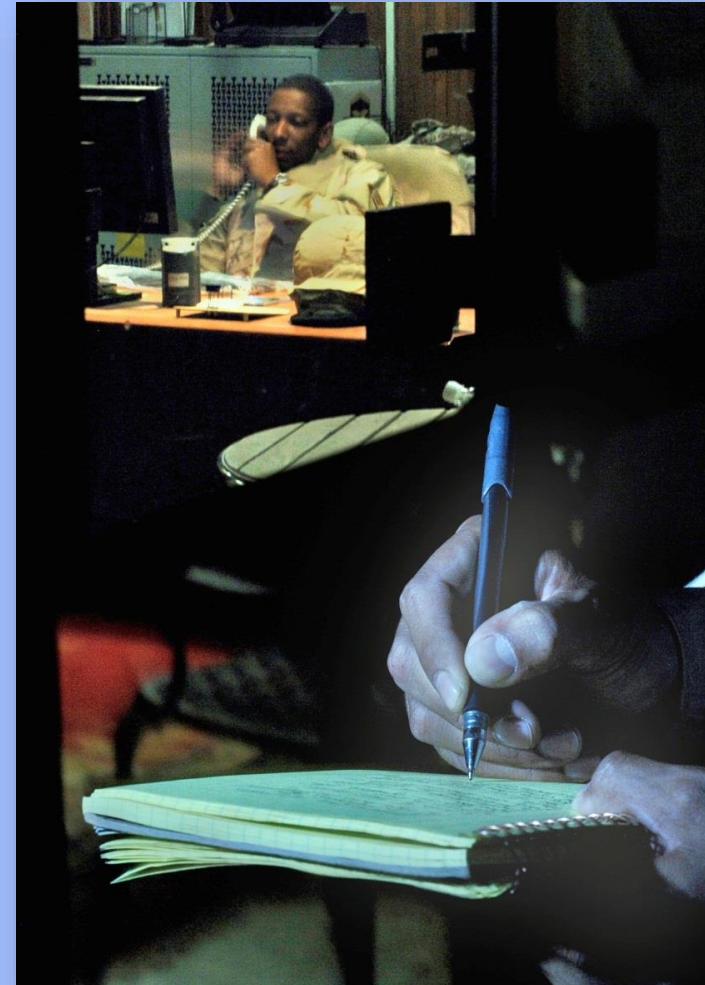


General Security

**OPSEC - Protect Information
about yourself and what you do.**

- Be alert.
- Support suspicious activity.

You are the first line of defense!





Travel Security

Complete required AT training.

Know locations of US Embassy.

Avoid use of rank or military affiliation on reservations or travel documents.

Travel on tourist passport.





Hotel Security

Upon entering your hotel room inspect the locks on the doors, windows, and safe.

Inspect the areas that could conceal a weapon or bomb such as the dresser and closet.





Tourism Safety

Research the potential threat conditions.

Don't travel alone.



Conceal your military affiliation.

Conform to local culture.

Avoid religious sites where your presence may be offensive.

Be aware of suspicious behavior.





In- Transit Security

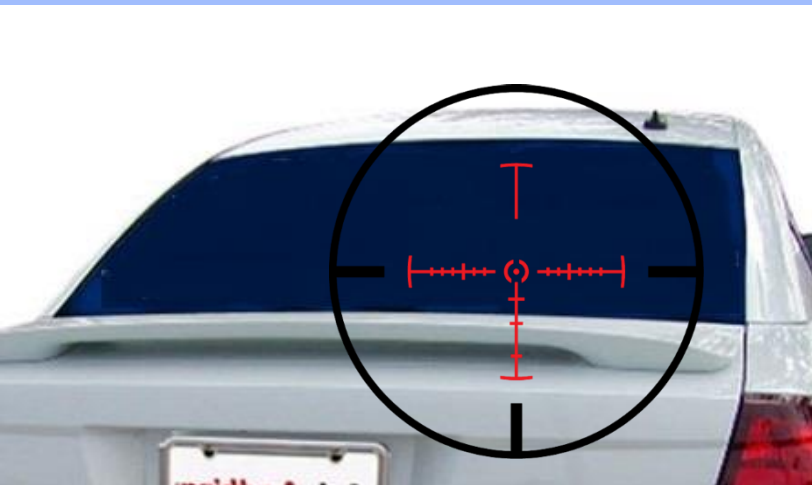
Check vehicle for tampering.

Keep vehicle secure.

Be unpredictable with routes and parking.

Maintain a low profile.

- Consider civilian clothing and
- Avoid car markings that can identify your affiliation.





In-Transit Security



Never touch Suspicious items!!



In-Transit Security

**Check traveler's tips from U.S.
Consulate Offices, travel agencies,
and websites.**

Think Security

Report suspicious activity





In-Transit Security



If you need to take a taxi during your trip, look for the distinctive markings of a legitimate taxi company.



Home Security



**Your Home
Your Security
Your Responsibility**





Home Security



- Locks
- Shrubbery
- Lighting
- Security systems





Home Emergencies

Post Emergency Numbers

Household Rules addressing Visitors

Emergency meeting place





Cyber Security

Don't give out your personal information!

Not on social media.

Not on chat.

Not on email.



Use antivirus software and a firewall.

Avoid using public computers.

If you suspect compromise of personal or official information, contact your security officer immediately.





Tips



Anonymity

Be Anonymous - Blend in, don't be an easily identified target.



Planning

Plan Ahead - Think ahead and choose safer options.



Awareness

Be Aware - Look for suspicious persons/activities.



Access

Control Access - Prevent crime, maintain security.



Unpredictability

Be Unpredictable - Change routines, routes, times, and speeds.



Teamwork

Be a Team Player - Cooperate with unit security measures.



ANG Total Force Awareness Training (TFAT)

Ancillary Refresher Program

Force Protection



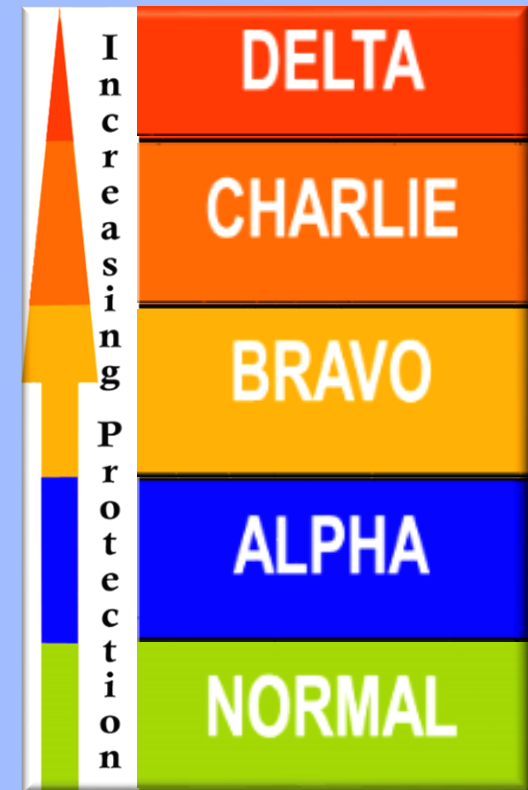


FPCON Levels

Force Protection Condition (FPCON) Levels

There are five FPCONs, beginning with Normal, then Alpha, and moving upward through Bravo, Charlie and Delta.

FPCON





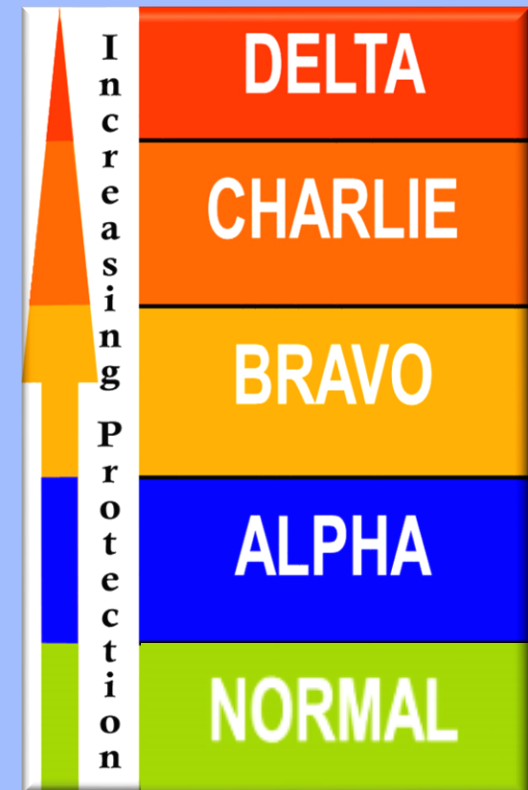
FPCON Levels

FPCON Normal

is a general threat of possible terrorist activity and you can expect to see a **routine base security posture**:



Expect to see a routine posture.





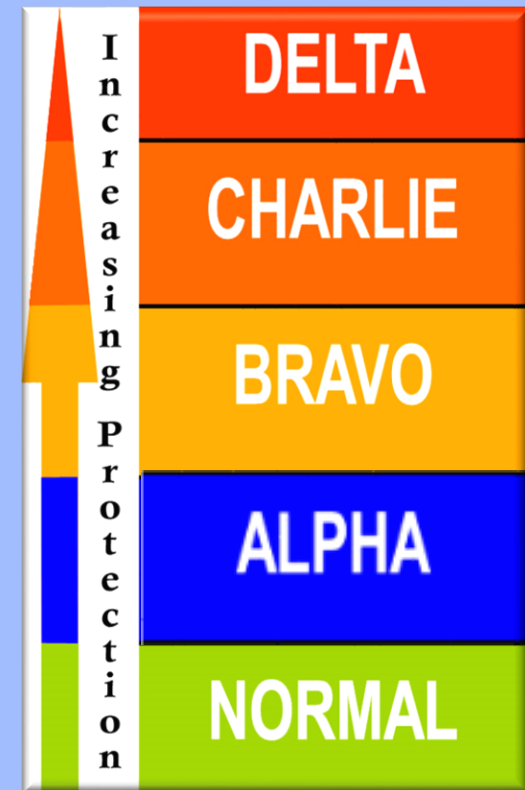
FPCON Levels

FPCON Alpha

When there is a general threat of **possible terrorist activity**, which are **unpredictable**, against personnel and facilities:



Expect random vehicle checks and increased crime prevention efforts.





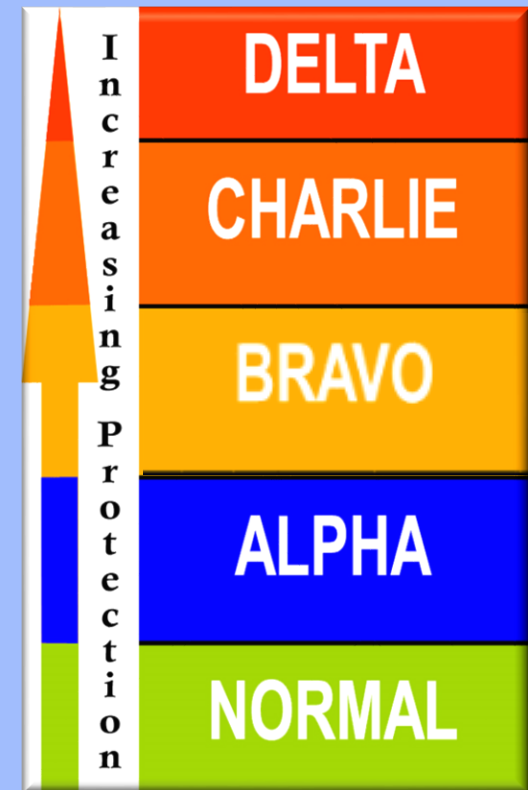
FPCON Levels

FPCON Bravo

When an increased and more **predictable terrorist threat activity** exists:



Expect to see closer inspection of vehicles and deliveries, ID checks, and a greater presence of guards on your installation.





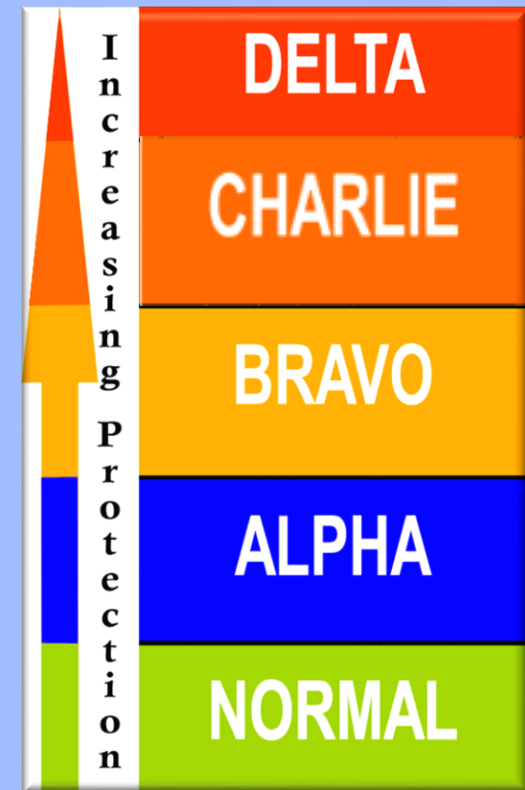
FPCON Levels

FPCON Charlie

When an incident occurs or when intelligence indicates that some form of **terrorist targeting against personnel and facilities** is imminent:



Expect increased inspections of vehicles and facilities and an increase in security forces augmentation.





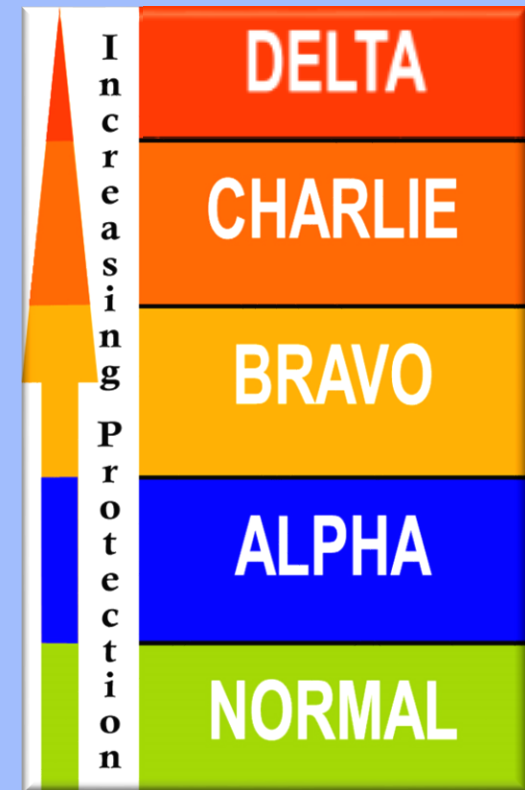
FPCON Levels

FPCON Delta

When an increased and more **predictable terrorist threat activity** exists:



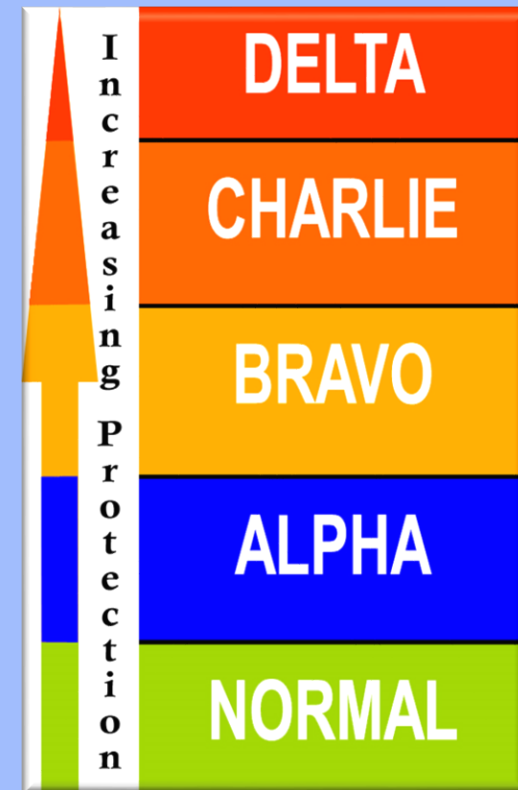
Expect an interruption or delay to normal installation routines.





Protective measures may include:

- Gate guards
- Barriers
- ID checks
- Vehicle inspections
- Patrols
- Plan rehearsals
- Random Antiterrorism Measures (RAMs)





ANG Total Force Awareness Training (TFAT)

Ancillary Refresher Program

Force Protection





Response to Threat Actions

Suspicious Activity or Persons

Always be on the lookout for suspicious activities or persons. If you see suspicious events or people report them immediately to security forces.





Response to Threat Actions

Suspicious or Unknown Package

Never accept a package, always call to confirm the package, delivery service provider, and sender.

If you receive an unexpected delivery to your hotel room, have the delivery left for you at the front desk.





Response to Threat Actions

Dealing with Terrorists

**DO NOT resist if confronted
with deadly force.**

Avoid escalating the situation.

Remain calm and respectful.

**Remember your Code of
Conduct training.**





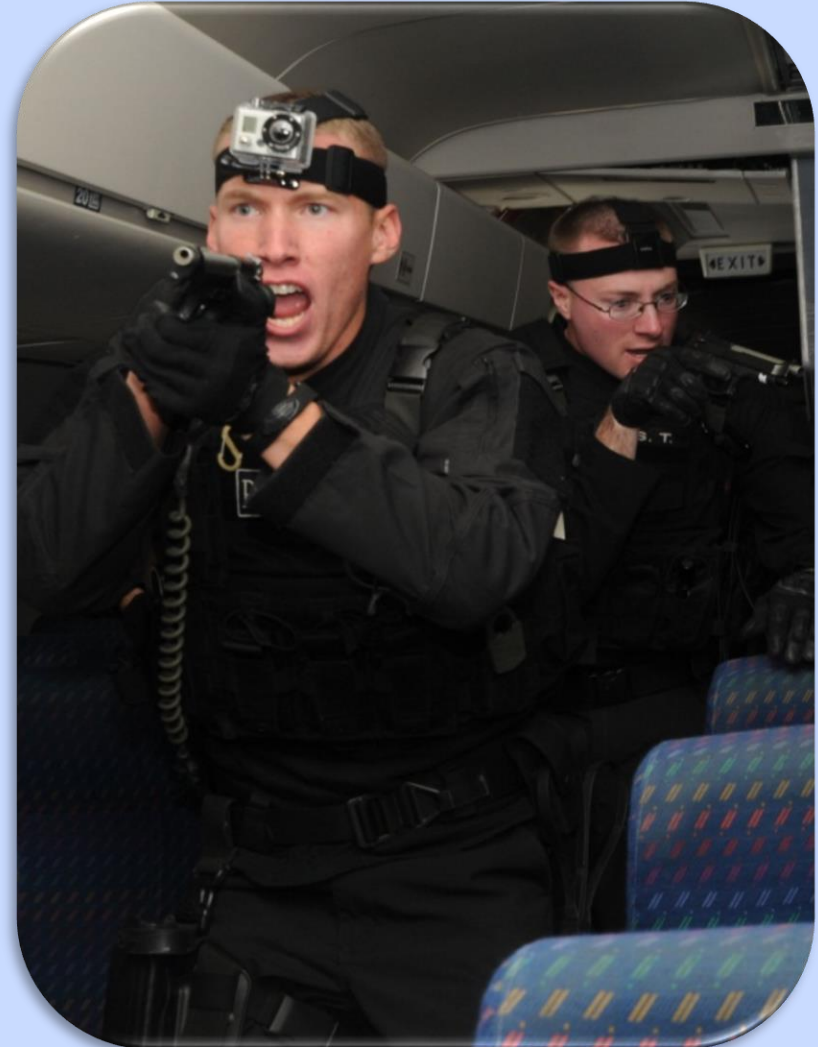
Airplane Hijacking

Stay alert & Remain calm

Don't identify yourself as a military member

Determine your best course of action based on the situation

You may have to respond to the threat.





Counter-Intelligence





Counter-Intelligence

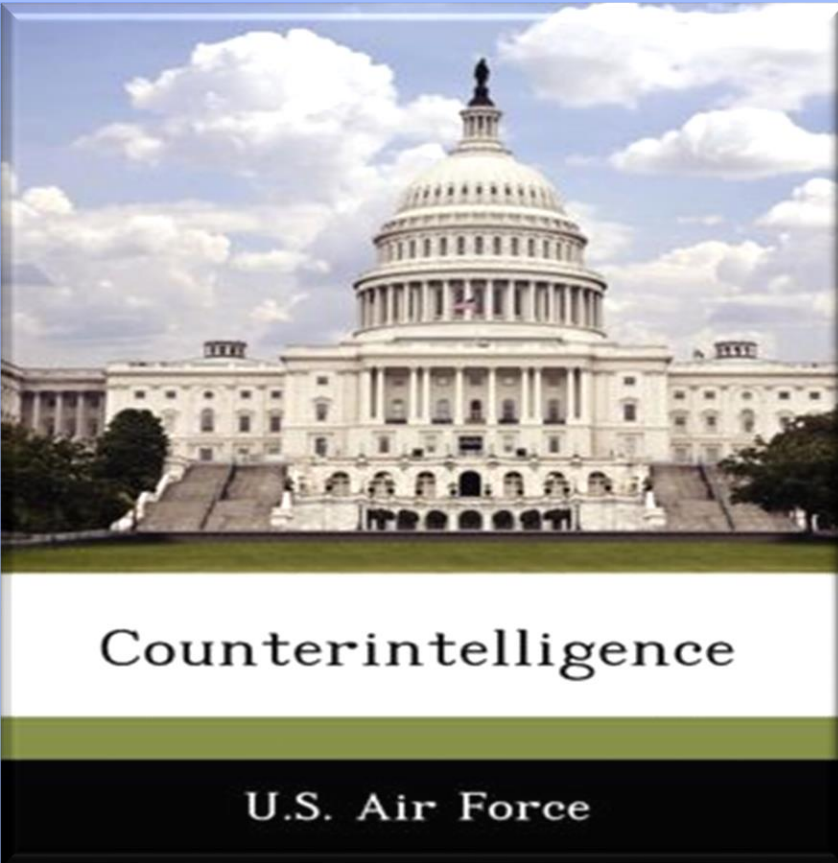
Critical Technological, industrial, and commercial information.

Intentions and targets of foreign intelligence services.

Neutralize the impact of espionage and sabotage



Intelligence



Intelligence encompasses functions involved in collecting, producing, and distributing data that have strategic, tactical, or technical value from and intelligence viewpoint.

Knowing what an adversary is doing, or plans to do, puts one in a much better strategic or tactical position.



Treason



Treason- Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort with the United States or elsewhere, is guilty of treason (see Title 18, USC. §2831).



Espionage



Espionage involves a government or individual obtaining information that is considered secret or confidential without the permission of the holder of the information.

Espionage is inherently clandestine, and is a subset of Intelligence gathering.



Sabotage



Sabotage is deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction.

In war, the word is used to describe the activity of an individual or groups actions result in the destruction or damaging of the productive or vital facility, such as equipment, factories, dams, public services, or logistic routes.



Subversion



Subversion is an act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline, of the Military Forces of the United States.



CI Threats

Traditional -- Hostile countries that openly target the United States

Non-Traditional -- threats today come in the form of terrorism, drug trafficking, serious communicable diseases, piracy, illegal immigration and information security.

Information Mercenaries -- Anyone who may seek intelligence information or access to the information for possible profit (i.e. Computer Hackers, Media, Aircraft Spotters, etc.)



Counterintelligence

CI incidents happen daily, and threats originate from various countries, groups, and individuals. The focus of the collection ranges from technological, to strategic, to terrorist.





Reportable Situations

You must report any of the following situations *immediately*:

Unauthorized contact with an individual who is suspected of being associated with a foreign intelligence/security organization, including attaches, or terrorist organization.

Illegal activity, conduct, or requests for participation in illegal activities or other conduct that might make someone susceptible to blackmail or result in security violation.



Reportable Situations

Individuals are required to report when unauthorized intrusion into U.S. automated information systems, networks, or other cyber capabilities, whether classified or unclassified;

Unauthorized transmissions of classified or unclassified controlled information without regard to

**Medium
Destination
Origin**

Must be reported to the AFOSI



Reportable Situations

Incidents or behaviors that are otherwise reportable must be reported to the supporting AFSOI or CI Office.

Remember, “contact” means any exchange of information directed to an individual including:

Solicited or Unsolicited Telephone calls

Text Messages

Interaction via social media

Networking websites

Email

Radio Contact

Face – to – face meeting and repeated contact with foreign national.



REMEMBER

**Counter-Intelligence is information gathered
(and activities conducted)
to protect against espionage and sabotage.**

Report any incidents or contacts to AFOSI *IMMEDIATELY*



Active Shooter



Questions?

This completes your yearly Force Protection Requirement. If you have any questions please reference the ANG SharePoint site:

<https://cs3.eis.af.mil/sites/OO-ED-AN-33/ANC/>