

ANTITERRORISM OVERVIEW



Force protection is the most important Installation priority. Leaders at all levels are expected to create a safe and secure environment for their Soldiers, DoD civilians, family members, and contractors and to remain personally involved in their force protection programs. Each member of Team Redstone must support the Antiterrorism program for it to succeed. We cannot risk the lives of our personnel by doing anything less than our very best to protect them.

Terrorism:

“The Calculated use of Violence or the Threat of Violence to Inculcate Fear; Intended to Coerce or to Intimidate Governments or Societies in the Pursuit of Goals that are Generally Political, Religious, or Ideological.”

Those acts are generally planned to attract widespread publicity and are designed to focus attention on the existence, cause or demands of the terrorists.

Antiterrorism:

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

Antiterrorism Awareness:

Fundamental knowledge of the terrorist threat and measures to reduce vulnerability to terrorism.

(FORCE PROTECTION CONDITIONS)

The Force Protection Condition system is mandated by the DoD & DA. FPCONS are progressive levels of security measures that are the foundation of all AT plans and orders.

FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. As a minimum, access control will be conducted at all DOD installations and facilities. The minimum FPCON for U.S. Army commands is NORMAL.

FPCON ALPHA applies when there is an increased general threat of possible terrorist activity against personnel or facilities, and the nature and extent of the threat are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.

NOTE: Expect traffic delays coming onto RSA due to increased Random Antiterrorism Measures. Special events with large gatherings may be postponed or cancelled.

FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration. **NOTE:** The installation will be on a lockdown and all activities will be curtailed or cancelled. Only Key Essential (KE) personnel and emergency vehicles will be allowed access to RSA during FPCON DELTA. The installation will resume normal operations once it is deemed safe.

It is important to understand that the FPCON system specifically designates “preventive actions, and responses to terrorist threats against U.S. personnel and facilities.” The FPCON system is NOT intended for use in developing actions and responses to other threats, such as crime, foreign intelligence threats, or political violence.

(RANDOM ANTITERRORISM MEASURES)

Are those additional security measures that are conducted at random dates, times and locations. RAM's are issued and tracked by the RSA AT Branch. An effective and robust RAM program will make our Installation a harder target and will provide unpredictable security patterns for our aggressors. RAMs are created from FPCON NORMAL through FPCON DELTA measures and any additional security measures the Threat Working Group deems necessary to detect or deter acts of terrorism.

iWATCH PROGRAM

Suspicious Person or Activity Reporting



iWATCH is a nationwide modern version of Neighborhood Watch developed by the Los Angeles Police Department to encourage and enable members of the community in identifying and reporting suspicious behavior that may be associated with terrorist activities. Army Senior Leadership has approved the Army's adoption of the **iWATCH** Antiterrorism Awareness Program. Team Redstone will implement the **iWATCH** program for all suspicious persons and activity reporting. The purpose of **iWATCH** is to promote antiterrorism awareness and leverage every member of the Team Redstone community to act as a sensor to help identify and prevent potential terrorist acts. There are two elements to the **iWATCH** program, *Passive* and *Active*. The *Passive* element of **iWATCH** is individual situational awareness of your surroundings. The *Active* element requires individuals to take action and report suspicious behavior or activities, to law enforcement for further investigation

Suspicious Vehicle Indicators

1. Rental vehicles/trailers parked near a facility, parked at or near the loading dock, or located in the parking lot without prior notification.
2. Appears to be overloaded or has any substance leaking from it.
3. Is parked illegally or parked at an unusual location.
4. Appears to be abandoned (e.g., inspection sticker expired or missing, registration plate expired or missing, etc).
5. Vehicle passing by key area/areas multiple times (e.g. possible surveillance).

Suspicious Person/Behavior Indicators

An Individual Observed:

1. Loitering near a facility or in the lobby of a facility for an extended period of time.
2. Wandering throughout a facility with no visible identification badge.
3. Dressed in oversized or inappropriate clothing (e.g.. A long heavy coat in warm weather) that appears to be concealing something.

4. Entering a facility carrying an oversized backpack or large suitcase.
5. Photographing, videotaping, and/or sketching the exterior or interior of any facility or installation area.
6. Who appears to be conducting surveillance of a facility (e.g.. Sitting in a vehicle for an extended period of time).
7. When challenged does not respond or does not provide a reasonable explanation.
8. Asking questions about key personnel and/or their activities.
9. Asking specific questions about a facility or the installation related to deployment and/or security matters.

Suspicious Item (s) Indicators

1. Any unattended backpacks, boxes, containers, luggage, and/or packages in an elevator, hallway, lobby, restroom, snack bar or stairwell of your facility.
 2. Any item that could be an improvised explosive device (e.g. items with visible wires, antennas, batteries, timing devices, metal or plastic pipe with each end capped or covered, etc.).
- NOTE: Untrained personnel should not examine or move a possible improvised explosive device (IED); the immediate area must be cleared pending the arrival of bomb squad personnel and the use of radios and/or cellular phones should be discontinued until the area has been cleared.

NOTE: Report all suspicious persons and activities to the Redstone Dispatch at (256) 313-6422. If you are at work please notify your supervisor and Organizational Antiterrorism Officer (ATO) once you have called the proper authorities. NOTE: If any incident appears life threatening call 911 immediately.

EMERGENCY ACTIONS

SUSPICIOUS PACKAGE/DEVICE

1. If you see an unattended package at any location, take the initiative and attempt to identify the owner. For example, if you see an unattended backpack or handbag at the Food Court that may have been forgotten or left behind, simply asking people in the immediate area may help to determine the owner. On the other hand, if it appears to be a suspicious package or has protruding wires, oily stains, is tightly taped, made of irregular packaging, or has foreign postmarks, there are steps that should be taken.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

2. When a suspicious package or device has been found, **DO NOT TOUCH IT**, report its location and general description immediately by calling 911 and ensure the facility supervisor/manager is notified.
3. The caller should be a minimum of 25 feet away from the suspicious package in order to prevent a possible electronic signal detonating the device. When reporting the package provide all details about the package - size, color, markings, exact location, etc.
4. Facility Supervisors/Managers should be prepared to evacuate the area around the discovery site if the object remains unexplainable.
5. Ensure the evacuated area is at least 100 meters from the suspicious object and provides adequate cover.
6. Keep individuals out of the area until Police arrive, and inform them of the objects location. Keep the person who located the object at the Incident Command Post (ICP) until the police have questioned them. Avoid re-entering the facility or area unless directed by police.
7. Suspected bombs/IEDs or incendiary devices will not be moved, jarred or touched by any organization personnel. Removal of these items will be conducted by EOD personnel only.

RECEIPT OF SUSPICIOUS ENVELOPE OR PACKAGE

SUSPICIOUS UNOPENED LETTER OR PACKAGE MARKED WITH THREATENING MESSAGE SUCH AS "ANTHRAX":

1. Do not shake or empty the contents of any suspicious envelope or package.
2. Place the envelope or package in a plastic bag or some other type of container to prevent leakage of contents.
 - a. If you do not have a container, **COVER** the envelope or package with anything (e.g., clothing, paper, trash can, etc.) and do not remove the cover.
 - b. Then **LEAVE** the room and **CLOSE** the door or section off the area to prevent others from entering (i.e., keep others away).
 - c. **WASH** your hands with soap and water to prevent spreading any powder to your face.
 - d. What to do next.
 - ✓ If you are at **HOME** report the incident to local police.

- ✓ If you are at **WORK**, call 911 and notify your Facility Manager or Supervisor.

3. **LIST** all people who were in the room or area when this suspicious letter or package was discovered. Give this list to both the local public health authorities and law enforcement officials for follow-up investigations.

ENVELOPE WITH POWDER AND POWDER SPILLS OUT ONTO SURFACE:

1. **DO NOT** try to **CLEAN UP** the powder. **COVER** the spilled contents immediately with anything (e.g., clothing, paper, trash can, etc.) and do not remove this cover!

2. Then, **LEAVE** the room and **CLOSE** the door, or section off the area to prevent others from entering (i.e., keep others away).

3. **WASH** your hands with soap and water to prevent spreading any powder to your face.

4. What to do next.

- ✓ If you are at **HOME** report the incident to local police.
- ✓ If you are at **WORK**, call 911 and notify your supervisor or Facility Manager.

5. **REMOVE** heavily contaminated clothing as soon as possible and place in a plastic bag, or some other container that can be sealed. This clothing bag should be given to the emergency responders for proper handling.

6. **SHOWER** with soap and water as soon as possible. Do Not Use Bleach Or Other Disinfectant On Your Skin.

7. If possible, list all people who were in the room or area, especially those who had actual contact with the powder. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

Emergency procedures

1. Turn off local fans or ventilation units in the area.

2. **LEAVE** area immediately.

a. **CLOSE** the door, or section off the area to prevent others from entering (i.e. keep others away).

b. What to do next.

- If you are at **HOME**, dial 911.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

- If you are at WORK dial 911 and notify your Supervisor or Facility Manager.

3. SHUT down air handling system in the building, if possible.

4. If possible, list all people who were in the room or area. Give this list to both the local public health authorities so that proper instructions can be given for medical follow-up, and to law enforcement officials for further investigation.

HOW TO IDENTIFY SUSPICIOUS PACKAGES AND LETTERS

Some characteristics of suspicious packages and letters include the following

- . Excessive postage
- . Handwritten or poorly typed addresses
- . Incorrect titles
- . Title, but no name
- . Misspellings of common words
- . Oily stains, discolorations or odor
- . No return address
- . Excessive weight
- . Lopsided or uneven envelope
- . Protruding wires or aluminum foil
- . Excessive securing material such as masking tape, string, etc.
- . Visual distractions
- . Ticking sound
- . Marked with restrictive endorsements, such as "Personal" or "Confidential"
- . Shows a city or state in the postmark that does not match the return address

NOTE: If you are off post call 911 and report the event.

BOMB THREATS

1. When receiving a telephonic threat, treat the call seriously. When a warning or threat is received complete the bomb-threat data card checklist located beside your phone and notify the Redstone Police or 911 immediately. Pretend you have difficulty with your hearing. If caller seems agreeable to further conversation, ask questions (listed on the checklist). **Note: All phones and work stations are required to have Bomb Threat Checklist.**

2. Be calm, be courteous, listen, and do not interrupt the caller. Notify other personnel that you have a bomb threat situation by waiving the bomb threat data card while the caller is still on line. That other person should immediately call 911.

3. Ask for information the caller does not provide, including the explosive device's location, time of detonation, etc. Secure and turn over written threats and the completed Bomb Threat Checklist to the Redstone Police.

4. Record all information given by the caller on the Bomb Threat Checklist. Keep the caller on the line as long as possible. Ask him/her to repeat the message. Do not hang up until the caller hangs up, and then immediately notify the Redstone police or 911. The J-911 Center may run a trace on the call after the incident depending on which trunk the call was received on. When calling 911 or the police state: "This is ' your name, organization and building number', we have a bomb threat and are evacuating the building".

5. Be prepared to make an announcement over the public address system or notification system once directed by the police and announce, "We have received a bomb threat at (give the location of the bomb if known) and all personnel are to evacuate the building and assemble in your pre-arranged assembly area".

THREATNING PHONE CALLS

Actions

Take all threatening calls seriously.

The most important reaction is to stay calm.

Stay in control. Carefully listen to what a threatening caller is saying. Take detailed notes such as the following:

Date:

Time:

Exact Words of Person Placing Call:

Caller's Identity: (*Male, Female, Adult, Juvenile,*)

Voice: (*Loud, Soft, High Pitch, Deep, Raspy, Pleasant, Intoxicated*)

Accent: (*Local, Not Local, Foreign*)

Speech: (*Fast, Slow, Distinct, Distorted, Stutter, Nasal, Lisp, Slurred*)

Language: (*Excellent, Good, Fair, Poor, Foul*)

Manner: (*Calm, Angry, Rational, Irrational, Coherent, Incoherent, Deliberate*)

Emotional: (*Righteous, Laughing, Intoxicated*)

Background Noises: (*Office Machines, Factory Machines, Trains, Animals, Music, Airplane*)

Other considerations

Don't make fun of a threatening caller or engage in personal attacks.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

If you get a threatening call, immediately report it to your supervisor, our safety director or another manager.

When necessary, call for outside emergency help. Call 911 if you ever think your life or the lives of others are in danger.

Security Managers and AT/FP persons should notify the Redstone Arsenal CID office of all threatening phone calls at 256 876-9682 or 256 876-2037.

DO:

Know our street address and location in case you need to call 911 or other outside emergency help.

Be sure the local police are notified in the case of a bomb threat. (Use the bomb threat checklist for all bomb threats)

DON'T:

Raise your voice or argue with a threatening caller.

Hang up on a caller making a bomb threat.

Hesitate to report any type of a threatening call to your supervisor or another manager.

ACTIVE ASSAILANT

Active Assailant (In Building): If you witness any armed individual shooting at people or hear gunshots inside the building verbally announce: "ACTIVE SHOOTER IN THE BUILDING" or "AN ACTIVE SHOOTER HAS ENTERED THE BUILDING". This must be loud enough to alert other work areas within the building. Individuals should continue to give the alarm to ensure the entire building has been notified.

Note: If it's possible to do safely, exit the building or area immediately when you become aware of an incident, moving away from the immediate path of danger, and take the following steps:

Run Tactic: If it's possible to do safely, exit the building or area immediately when you become aware of an incident, moving away from the immediate path of danger, and take the following steps:

1. Evacuate to a safe area away from the danger and take protective cover (Avoid parking lots and areas that do not provide adequate cover or concealment).

2. Notify anyone you may encounter to exit the building or area immediately (**DO NOT ACTIVATE THE FIRE ALARM**)

3. Call 911 and provide the dispatcher the following information. **NOTE:** Madison County 911 will answer calls when calling 911 from a cell phone on post. Be sure to tell them your specific location.

- a. State your name and that you are reporting an Active Shooter Incident
- b. Location of the Incident (be as specific as possible)
- c. Number of Shooters if Known
- d. ID or description of person
- e. Type of weapons used if known
- f. Your exact location
- g. Injuries to anyone if known

4. Individuals not immediately impacted by the situation are to take protective cover, staying away from the windows and doors until notified to do otherwise.

Hide/Barricade Tactic: If you are directly involved in an incident and exiting your building is not possible, the following actions are recommended:

1. Go to the nearest room or office then close and lock the door (Do not stay in the open hall)

2. Turn off the lights

3. Seek protective cover and stay away from doors and windows and Barricade yourself in the room. Move heavy objects to barricade the door. If barricading the door with objects in the room is not possible, use objects in the room as obstacles to slow down, fix, turn, or obscure the vision of the shooter. Even though an obstacle will not prevent a shooter from entering your work area it will help you achieve a tactical advantage to "Defend Your Sector." The phrase "Defend Your Sector" simply implies the actions taken during the fight to protect yourself and others in the area where you barricaded yourself.

4. Hide in a place that reduces observation from the shooter, but allows you to react if you must defend your sector.

5. These positions should provide cover and/or concealment. Cover is an object which protects you from weapons fire. Concealment protects you from enemy observation.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

6. Keep quiet and act as if no one is in the room. Turn off any audio equipment.
7. Do not answer the door unless you are positive it's not the shooter(s).
8. Call 911 or the Redstone Police Desk at 876-2222. (See previous page for details)
9. Place your cell phone on silent or vibrate and wait for police to assist in evacuation.
10. Once first responders make contact with you communicate with response forces as necessary.

Fight Tactic: Hopefully by now leaders have effectively leveraged the recommendations outlined in Active Shooter Awareness and Resilience training to properly condition their employees to react to a hostile threat. To clarify, fight is not a last option. As with each tactic previously discussed, fight is employed when it offers you the best chance for survival. Fight may be your first and only option. You would choose to fight if: (1) you are directly confronted with the shooter(s) or (2) the shooter(s) breaches your barricade and you need to defend your sector. In short, if you are directly engaged with a hostile force or engagement is imminent; your best chance for survival is to counter the threat with fight. As already stated, even if you select run and hide/barricade you must always be prepared to transition to fight if the tactical situation changes. It is important to note, pursuit of an active shooter(s) is discouraged with the exception being armed security forces. However, violent and fierce fight for survival is advocated when the tactical situation dictates. Your ability to fight will greatly be affected by your weapon status (i.e., armed or unarmed) and your ability to engage with surprise, speed, and violence of action. The following are considerations that enhance your chances of survival when employing fight:

1. Secure an improvised weapon (e.g., something to strike or throw).
2. Throw objects aiming at the individual's head (surprise); followed by an immediate (speed) committed counter attack (violence of action).
3. Attempt to disarm or direct the weapons away from you and others.
4. Commit to the fight. There is no move that is "off limits." Use whatever is necessary to survive and incapacitate the shooter(s). Hit the shooter with an object or fist, eye gouge, bite, groin strike, pull hair,

stomp on feet, head butt, punch individual in the throat (violence of action). Whatever it takes, become more violent than the shooter and do not stop until the threat is subdued or terminated.

5. Focus attacks on weak points in the shooter's defense: eyes, nose, groin, throat and hit hard, hit fast, and hit often.
6. Seize the initiative. If you are directly in the vicinity of the shooter(s) and your fellow employee attacks the shooter(s), join the fight and overwhelm the shooter(s). Do not stop your attack until the shooter has been rendered incapable of continuing their act of violence. Evident by the actions of United Airlines Flight 93 a small number of unarmed individuals can overrun an armed individual in a singular united effort if they exploit surprise, speed, and violence of action.

Other considerations

1. No matter what the circumstances, if you decide to flee during an active shooting situation, make sure you have an escape route and plan in mind.
2. Do not attempt to carry anything while fleeing. Move quickly, **keep your hands visible**, and follow the instructions of any police officers you encounter.
3. Do not attempt to remove injured people. Instead, leave wounded victims where they are and notify authorities of their location as soon as possible.
4. Do not try to drive off until released by police or supervisors.

SHELTER IN PLACE FOR CBRN EVENT

1. Sheltering in place during a chemical, biological, radiological, or nuclear (CBRN) event requires additional actions than those for severe weather shelter-in-place, to include:
 - If possible, turn off all air handling equipment (heating, ventilation, and/or air conditioning). **Ensure location of all Emergency HVAC shutoff switches are identified in the EAP**
 - Shut and lock all exterior windows and doors.
 - Close all interior doors.
 - Move to designated CBRN Shelter in Place location identified in the plan. **Ensure rooms are marked and identified in the EAP.**
 - Tape seal and tape all doors and vents in SIP location. **Ensure SIP kits are readily available or prepositioned in rooms.**

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

- When the “all clear” is announced, open windows and doors, turn on ventilation systems and have occupants go outside until the building’s air has been exchanged with the outside air.
- Get personnel accountability.

2. Civilians cannot be required to shelter-in-place. Therefore, it is important to develop your shelter in place plan with employees to maximize their cooperation with the shelter plan. Military personnel can be required to shelter-in-place.

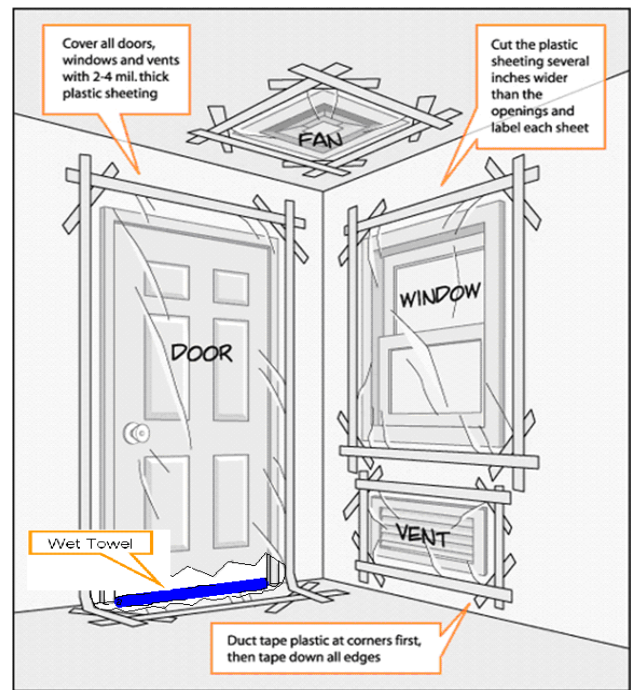
3. Develop a plan so that employees who wish to leave may do so by a door that will not endanger those who shelter-in-place. Determine if all employees will shelter or if some will leave the building before shelter procedures are put in place. If possible, designate one door for exiting and entry during the shelter-in-place for CBRN incidents.

4. Notification should come from redundant means ranging from e-mail notifications from the IEOC to Installation 24/7 and Emergency Action Officers (EAOs), local radio and television stations, and Giant Voice speaker systems.

5. **Shelter in Place Location:** The room should be above ground level as most Toxic Industrial Chemicals/Toxic Industrial Materials are heavier than air and the room should have as few windows, doors and vents as possible. The room should also provide about 10 square feet of floor space per person; so a facility with a work force of 10 people should have a SIP room that is at least 100 square feet. Other bonus features are access to a rest room, land line, TV, and a water supply. These items are not required and are merely a convenience.

6. **Shelter in Place Kits:** Once a location has been chosen, a SIP kit should be put together. This kit should contain plastic sheeting (one pre-cut sheet for every SIP room opening) and the plastic should be of durable quality and not plastic garbage bags which can have inconsistencies from the manufacturing process. It's best to label the sheets according to the location they'll be taped to for quick and easy application during an emergency. Extra inches should be added to each piece to ensure the piece can be taped to a flat wall if possible. Additionally, the kit should have duct tape and scissors, a first aid kit, flashlight with batteries, some sort of communication device - this may be a cell phone, LMR, or land line - a non-airtight box to keep the items in (an airtight box could produce mold by holding moisture in), shelter-in-place procedures, water, inventory and inspection sheet.

HOW TO PROPERLY SEAL A ROOM



Be sure to review your facilities Emergency Action Plan to become more familiar with your facilities lockdown procedures to include designated shelter and assembly area locations. Contact your Facility Manager, EM Coordinator or ATO for details.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

TRAVEL TIPS

Learn your destination: Find Country Specific Information, Travel Alerts, and Travel Warnings. Visit

<https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html>

The Department of State (DOS) issues a Travel Advisory for each country of the world. Travel Advisories follow a consistent format and use plain language to help U.S. citizens find and use important security information. Travel Advisories apply up to four standard levels of advice, give a description of the risks, and provide clear actions U.S. citizens should take to help ensure their safety.

Level 1 - Exercise Normal Precautions: This is the lowest advisory level for safety and security risk. There is some risk in any international travel. Conditions in other countries may differ from those in the United States and may change at any time.

Level 2 - Exercise Increased Caution: Be aware of heightened risks to safety and security. The Department of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

Level 3 - Reconsider Travel: Avoid travel due to serious risks to safety and security. The Department of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

Level 4 - Do Not Travel: This is the highest advisory level due to greater likelihood of life-threatening risks. During an emergency, the U.S. government may have very limited ability to provide assistance. The Department of State advises that U.S. citizens not travel to the country or to leave as soon as it is safe to do so. The Department of State provides additional advice for travelers in these areas in the Travel Advisory. Conditions in any country may change at any time.

NOTE: Travel Advisories at Levels 2-4 will contain clear reasons for the level assigned, using established risk indicators and specific advice to U.S. citizens who choose to travel there.

DoD persons traveling overseas must review the Foreign Clearance Guidance and Combatant Commander Travel guidance by accessing <https://www.fcg.pentagon.mil/fcg.cfm>

Enroll in to the Smart Traveler Enrollment Program: The Smart Traveler Enrollment Program (STEP) is a free service to allow U.S. citizens and nationals traveling abroad to enroll their trip with the nearest U.S. Embassy or Consulate.

Visit <https://travel.state.gov/content/passports/en/country.html>

Check-in with your doctor and insurance carrier. Double check and make sure that you have all of the proper vaccinations and that you have renewed all essential prescriptions. Also, ask your medical insurance provider if your policy applies overseas for emergencies. If it doesn't, and you want to add extra coverage.

Plan your wardrobe: Travel in conservative civilian clothing when using commercial transportation or when traveling in military airlift if you are connecting with a flight at a commercial terminal in a high-risk area.

Make sure your credit card will work in the country you're visiting. European banks have switched almost completely to the more secure chip-and-PIN technology, and fewer businesses abroad are accepting the outdated magnetic-strip cards.

Make copies of your passport, airplane ticket, driver's license, and credit cards.

Do not take unnecessary identification or credit cards.

Establish points of contact:

Ensure family members learn a duress word and it is on file at your office.

Advise associates or family members of your destination and anticipated time of arrival.

Take any necessary medications.

Activate your phone's global capabilities. There's usually a charge for doing this, but it is much less than the roaming charges you'll get if you don't.

COMMUTING/LOCAL TRAVEL

Look for tampering. Look under and around your auto.

At all times, keep your doors locked and windows rolled up.

Alter routes and avoid choke points.

Alternate parking places.

Plan safe locations along your route.

Redstone Arsenal Antiterrorism Awareness Desk reference as of 31 July 2019

DURING YOUR STAY

Be courteous and cooperative when processing through customs. Do not leave your bags unattended. Stay alert.

Use authorized taxis. You could be overcharged, robbed or kidnapped when using “gypsy” taxis

Do not leave drinks unattended – someone could slip a drug into it that causes amnesia and sleep.

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate.

Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.

ROOM SECURITY

Select an inside hotel room (away from the street-side window), preferably on the 4th–10th floors.

Keep doors and windows locked at all times.

Use peephole viewers before you open the door. Don't open the door to anyone until you know who it is.

EMPLOYEE RESOURCES

Installation HOT LINE: 1-877-863-1462

If a natural or manmade disaster causes RSA to close or delay opening, the announcement will be provided by the local media:

TV- CH 31/WAAY, CH 19 WHNT, CH 48 WAFF, CH 54 WZDX

FM RADIO- 99.1 FM, 102 FM, 90.9 FM, 100.3 FM, 106.1 FM, 89.3 FM, 90.9 FM, 104.3 FM

AM RADIO- 770 AM, 1050 AM, 1240 AM, 1270 AM, 1600 AM

"Download the Redstone Explorer Mobile Application to receive alerts and news at Google and Apple Stores"

Social Media Sites (Team RSA internet site):

<https://www.home.army.mil/redstone>

www.facebook.com/TeamRedstone

www.twitter.com/TeamRedstone

Important Telephone Numbers:

RSA Police Desk: 256-876-2222 (non-emergency)

RSA Installation Emergency Operation Center:
256-313-1043

RSA Physical Security: 256-876-6815/ 9998

RSA J911 Non-Emergency number (256) 313-6422