

**A Self-Help Guide to  
ANTITERRORISM**



**10 June 2013**

(INTENTIONALLY BLANK)

CJCS Guide 5260

“A Self-Help Guide to Antiterrorism”

10 June 2013

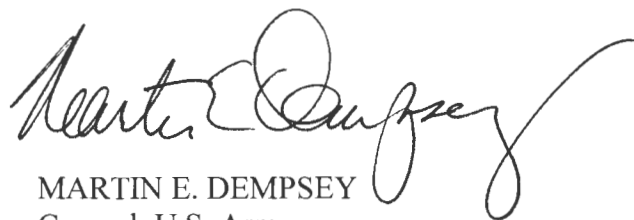
---

**FOREWORD**

The men and women who serve in the Department of Defense (DoD), together with their family members, are our most vital resource. As recent events have shown, terrorists have reached new levels of organization, sophistication, and violence, often targeting DoD personnel and their families. Their tactics and techniques are always changing and will continue to be a challenge to predict and neutralize. Accordingly, we must remain diligent in applying the proper protective measures.

Use of this guide and these proven security habits will not ensure immunity from terrorist attacks but should reduce the possibility of becoming a target. Defensive awareness and personal security are responsibilities of everyone assigned to DoD. Your overall awareness will not only help to protect your family but will also increase the security of all members of the military family.

This guide is designed to assist in making you and your family less vulnerable to terrorists. It is important that you ensure all members of your family are made aware of this valuable information so they not only protect themselves, but also become an integral part of the overall community antiterrorism effort. Constant awareness will help protect all members of the military family from acts of terrorism.



MARTIN E. DEMPSEY  
General, U.S. Army  
Chairman of the Joint Chiefs of Staff

18

(INTENTIONALLY BLANK)

# CJCS Guide 5260

## TABLE OF CONTENTS

	Page
Section I	
General Security Checklist .....	1
Home and Family Security .....	2
Alert Systems.....	8
Household Security Checklist.....	10
Operations Security Guidance for Family Members .....	12
Ground Transportation Security .....	14
Tips for Defensive Air Travel.....	18
Tips for Active Shooter Response .....	22
Responding to Chemical Threats.....	25
Responding to Biological Threats .....	27
Responding to Radiological Threats.....	29
Section II	
Guidance for Isolated Personnel .....	31
Pre-Mission Isolation Planning.....	34
Recovery .....	37
Captivity .....	39
Guidance for Detention by Hostile Governments (Detainee).....	46
Guidance for Detention by Terrorists (Hostage) .....	47
Taken Hostage -- You Can Survive! .....	48
Personal Data.....	50
Antiterrorism Points of Contact.....	54

Note: This document supersedes CJCS Guide 5260, 1 September 2010.

Releasability: This directive is approved for public release; distribution is unlimited. DOD Components (to include the combatant commands), other Federal agencies, and the public, may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <[http://www.dtic.mil/cjcs\\_directives](http://www.dtic.mil/cjcs_directives)>

(INTENTIONALLY BLANK)

**Section I**

---

---

**General Security Checklist**

- Keep a low profile. Your dress, conduct, and mannerisms should not attract attention. Make an effort to blend into the local environment. Avoid wearing expensive jewelry. Avoid publicity and do not go out in large groups. Stay away from civil disturbances and demonstrations.
- Be unpredictable. Vary daily routines, such as your route to and from work and the time you leave and return home. Vary the way you dress. Do not exercise at the same time and place each day. Never exercise alone, on deserted streets or country roads.
- Be alert for anything suspicious or out of place. Do not give personal information over the telephone. If you think you are being followed, go to a pre-selected secure area such as a military base or police station. Immediately report the incident to the military police, security forces, or law enforcement agencies. In overseas areas without such agencies, report suspicious incidents to the security officer or the military attaché at the U.S. Embassy. Instruct your family and associates not to provide strangers with information about you or your family.
- Report all suspicious persons loitering near your office or in unauthorized areas. Attempt to provide a complete description of the person and/or vehicle to police or security personnel.
- Advise associates or family members of your destination and anticipated time of arrival when leaving the office or home.
- Do not open doors to strangers and report unsolicited contacts to authorities. Refuse to meet with strangers outside your work place.
- Pre-program cell phones and memorize/write down key phone numbers -- office, home, police, security, etc.
- When overseas, always know the location of the nearest U.S. Embassy, Consulate, or military organization.
- Be cautious about giving out information regarding family travel plans or security measures and procedures.
- When overseas, learn and practice a few key phrases in the local language, such as “I need a police officer/doctor.”

## Home and Family Security

You and your family members should always practice basic personal security precautions. Familiarize your family with the local terrorist and criminal threat and regularly review the protective measures and techniques listed in this handbook. Ensure everyone in your family knows what to do in case of emergency.

In addition to installation-specific Web sites, the following Web sites may also provide useful information about recent threats or activities. Indeed, portions of this guide are derived from the sources below.

In the continental United States (CONUS):

- U.S. Department of Homeland Security  
<http://www.dhs.gov> and <http://www.ready.gov>
- Federal Emergency Management Agency  
<http://www.fema.gov>
- The American Red Cross  
<http://www.redcross.org>
- Centers for Disease Control and Prevention  
<http://www.bt.cdc.gov> and <http://emergency.cdc.gov>

Overseas:

- U.S. Department of State  
<http://travel.state.gov> or <http://www.state.gov>  
Also, the Department of State has a travel registry for U.S. citizens living or traveling overseas. Called STEP (Smart Traveler Enrollment Program), this service is used to facilitate contact between the local U.S. Embassy or Consulate and the individual during times of emergencies. More information on the process can be found at: <https://travelregistration.state.gov>
- National Center for Medical Intelligence (SIPRNET Site for Health Threats)  
<http://www.afmic.dia.smil.mil>

Service personnel and DoD civilians can find classified regional assessments and updates through the DoD Foreign Clearance Guide Web site (<http://www.fcg.pentagon.smil.mil>). Unclassified assessments can be found at <https://www.fcg.pentagon.mil>. Combatant commander Web sites will also have links to current information.

USNORTHCOM: INTERNET -- <http://www.northcom.mil>  
SIPRNET -- <https://operations.noradnorthcom.smil.mil>

USEUCOM: INTERNET -- <http://www.eucom.mil>  
SIPRNET -- <https://portal.eucom.smil.mil>



USSOUTHCOM: INTERNET -- <http://www.southcom.mil>  
 SIPRNET -- <http://www.southcom.smil.mil>

USCENTCOM: INTERNET -- <http://www.centcom.mil>  
 SIPRNET -- <https://rel.centcom.smil.mil/>

USPACOM: INTERNET -- <http://www.pacom.mil>  
 SIPRNET -- <http://www.pacom.smil.mil>

USAFRICOM: INTERNET -- <http://www.africom.mil>  
 SIPRNET -- <https://portal.africom.smil.mil>

Further information on the local terrorist threat can be obtained through your chain of command from your antiterrorism officer (ATO) or command intelligence officer.

### **TRAINING**

DoD AT policy requires all DoD personnel, to include dependent family members ages 14 years and older, to complete Level I Antiterrorism Awareness Training if they are traveling outside CONUS as part of official orders or permanent change of station. Level 1 AT Awareness Training is available on the NIPRNET at <https://atlevel1.dtic.mil/at/>.

Every Geographical Combatant Command mandates that personnel entering their area of operations for duty purposes complete SERE 100.1 training as part of their theater entry requirements. SERE 100.1 training is available on the SIPRNET at <http://intelshare.intelink.sgov.gov/sites/jko/default.aspx> or on the NIPRNET at <http://jko.jfcom.mil/index.html>.

### **TIPS FOR THE FAMILY AT HOME**

- Restrict the possession of house keys. Change locks if keys are lost or stolen and when moving into a previously occupied residence.
- Lock all entrances at night, including the garage. Keep the house locked, even if you are at home.
- Destroy all envelopes or other items that show your name, rank, or other personal information. Remove names and rank from mailboxes.
- Maintain friendly relations with your neighbors.
- Do not draw attention to yourself; be considerate of neighbors.
- Keep yourself informed via media and internet regarding potential threats.
- Develop an emergency plan and an emergency kit, including a flashlight, battery-operated radio, first-aid kit including latex gloves, and copies of important personal documents including key points of contact.

### **BE SUSPICIOUS**

- Be alert to public works crews and other individuals requesting access to your residence; check their identities through a peephole or contact the parent company to verify employee status before allowing entry.

- Be cautious about peddlers and strangers, especially those offering free samples. Do not admit salespersons or poll takers into your home.
- Watch for unfamiliar vehicles cruising or parked frequently in the area, particularly if one or more occupants remain in the vehicle for extended periods.
- Write down license plate numbers, makes, models, and colors of suspicious vehicles. Note descriptions of occupants.
- Report any suspicious videotaping/photography or unusual accommodation requests.
- Report any unattended bags or objects.
- Treat with suspicion any inquiries from strangers concerning the whereabouts or activities of family members.
- Report all suspicious activity to military police, security forces, or local law enforcement as appropriate.

### **TELEPHONE SECURITY**

- Post emergency numbers on the telephone and pre-program phone numbers where possible.

- Military Police/Security Forces: \_\_\_\_\_
- U.S. Embassy: \_\_\_\_\_
- Local Police: \_\_\_\_\_
- Fire Department: \_\_\_\_\_
- Hospital: \_\_\_\_\_
- Ambulance: \_\_\_\_\_

- Do not answer your telephone with your name and rank.
- Report all threatening phone calls to security officials and the telephone company. Attempt to ascertain any pertinent information about the caller to include background noise, accent, nationality, or location.

### **WHEN TRAVELING**

- Travel in small groups as much as possible and vary movements so as not to be predictable.
- Try to be inconspicuous when using public transportation and facilities. Dress, conduct, and mannerisms should not attract attention and be generally similar to that worn by the people in the area.
- Avoid spontaneous gatherings or demonstrations.
- Stay away from known trouble, disreputable places, or other high-risk areas. Visit reputable establishments. Efforts should be made to avoid known U.S.-associated locales overseas. The U.S. Embassy Regional Security Officer should be able to provide a list of areas to be avoided. Travelers should first review the consular information sheet for the particular country as this serves as the principal means for

disseminating safety, health, and security information for travelers. These are available at [www.travel.state.gov](http://www.travel.state.gov).

- Know emergency numbers and how to use the local telephone system.
- Ensure family members have a list of phone numbers they can carry with them at all times. The list should not outline titles, positions, or office locations but should be usable during an emergency.
- Do not discuss travel plans, detailed family issues, or office plans over the telephone.
- When using hotels:
  - Place the “do not disturb” sign on the door and consider leaving the lights and television on when departing the room.
  - Keep room key cards hidden on your person so you do not reveal the hotel you are using.
  - Avoid rooms on the first two floors and those facing streets as they receive more impact from street level blasts. Rooms on the lower floors and rooms that are accessible from outside the hotel also tend to be more vulnerable to unauthorized entry.
  - If possible, avoid rooms above the seventh floor as fire and rescue equipment may not be able to reach higher levels.

#### **SPECIAL PRECAUTIONS CONCERNING CHILDREN**

- Never leave young children alone or unattended. Be certain children are in the care of a trustworthy person.
- If it is necessary to leave appropriately aged children at home (consistent with local command guidance), keep the house well lighted and notify a trusted neighbor.
- Instruct children to keep doors and windows locked and to not allow strangers inside.
- Teach children how to contact the police or neighbor in an emergency.
- Ensure children know where and how to contact parents at all times.
- Maintain recent photographs of your children. The photographs should display a clear view of the child’s head.
- If you have children entering the home alone, teach them not to enter the home if the door is ajar, if a strange car is in the driveway, or if something else does not seem right. Tell them where they need to go if this situation occurs.
- Instruct your children to:
  - Never leave home without telling you where they will be and who will accompany them.
  - Travel in pairs or small groups.
  - Avoid isolated areas.

- Use locally approved play areas where recreational activities are supervised by responsible adults and where police protection is readily available.
- Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot even if the strangers say mom or dad sent them, or said it was “okay.” Children should similarly be aware of strangers offering gifts, food, or using small animals to get them into a vehicle.
- Report immediately to the nearest person of authority (parent, teacher, or police) anyone who attempts to talk to or touch them in any way that makes them feel uncomfortable or scared.
- Never give information about family members over the phone, e.g., parent’s occupation, names, or future family plans and dates.
- Screen phone calls through voice mail to avoid answering calls from strangers.

### **SECURITY PRECAUTIONS WHEN YOU ARE AWAY**

- Leave the house with a lived-in look (i.e. cut the grass and trim hedges before leaving).
- Stop deliveries of newspapers and mail or forward to a trusted neighbor’s home. Mail can also be held at the post office.
- Do not leave notes on doors or indicate the length of absence on telephone voicemail or electronic mail account.
- Do not hide keys outside the house.
- Use a timer to turn lights on and off at varying times and locations.
- Consider leaving the radio and lights on.
- Hide valuables.
- Notify the police or trusted neighbor of your absence.
- Ask a trusted friend or neighbor to check the residence periodically.

### **SUSPICIOUS PACKAGES OR MAIL**

- Suspicious characteristics to look for include:
  - Unusual or unknown place of origin.
  - No return address.
  - Excessive amount of postage.
  - Abnormal or unusual size or shape.
  - Protruding strings, aluminum foil, or wires.
  - Misspelled words.
  - Differing return address and postmark.
  - Handwritten labels, foreign handwriting, or poorly typed addresses.

- Unusual odor. (Deliberate or sustained smelling of a piece of mail to determine the existence of an unusual odor is not advised; this could expose you to chemical or biological agents.)
  - Unusual or unbalanced weight, either heaviness or lightness.
  - Springiness in the top, bottom, or sides.
  - Inflexibility.
  - Crease marks, discoloration, or oily stains.
  - Incorrect titles or title with no name.
  - Excessive security material, such as masking tape, string, etc.
  - Ticking, beeping, or other sounds.
  - Marked with special instruction such as “Personal,” “Rush,” “Do Not Delay,” or “Confidential.”
  - Evidence of contamination, such as a powdery substance that is out of place in the package or not normally received from the sender.
- The lack of the above indicators does not guarantee the package is safe. Use your best judgment.
  - Do not handle suspicious packages unnecessarily. Never cut tape, strings, or other wrappings on a suspect package or immerse a suspected letter or package in water. Such action could cause an explosive device to detonate.
  - If the object has already been moved, place the letter or package in a plastic bag or some other container to prevent leakage of contents. If you are not certain whether a package or letter has been moved, avoid touching or moving it.
  - If handling mail suspected of containing chemical or biological contaminants, wash hands thoroughly with soap and water.
  - Make a list of personnel who were in the room or area when the suspicious envelope or package was recognized.
  - Report any suspicious mail or packages to security officials immediately. Isolate the item if possible.

## Alert Systems

The Force Protection Conditions (FPCON) system describes the progressive level of protective measures implemented by DoD installations or units in response to terrorist threats. There are five FPCON levels. Each level has separate supporting measures that incrementally raise preparedness and protection capabilities. Figure I provides a general description of the circumstances surrounding each FPCON.

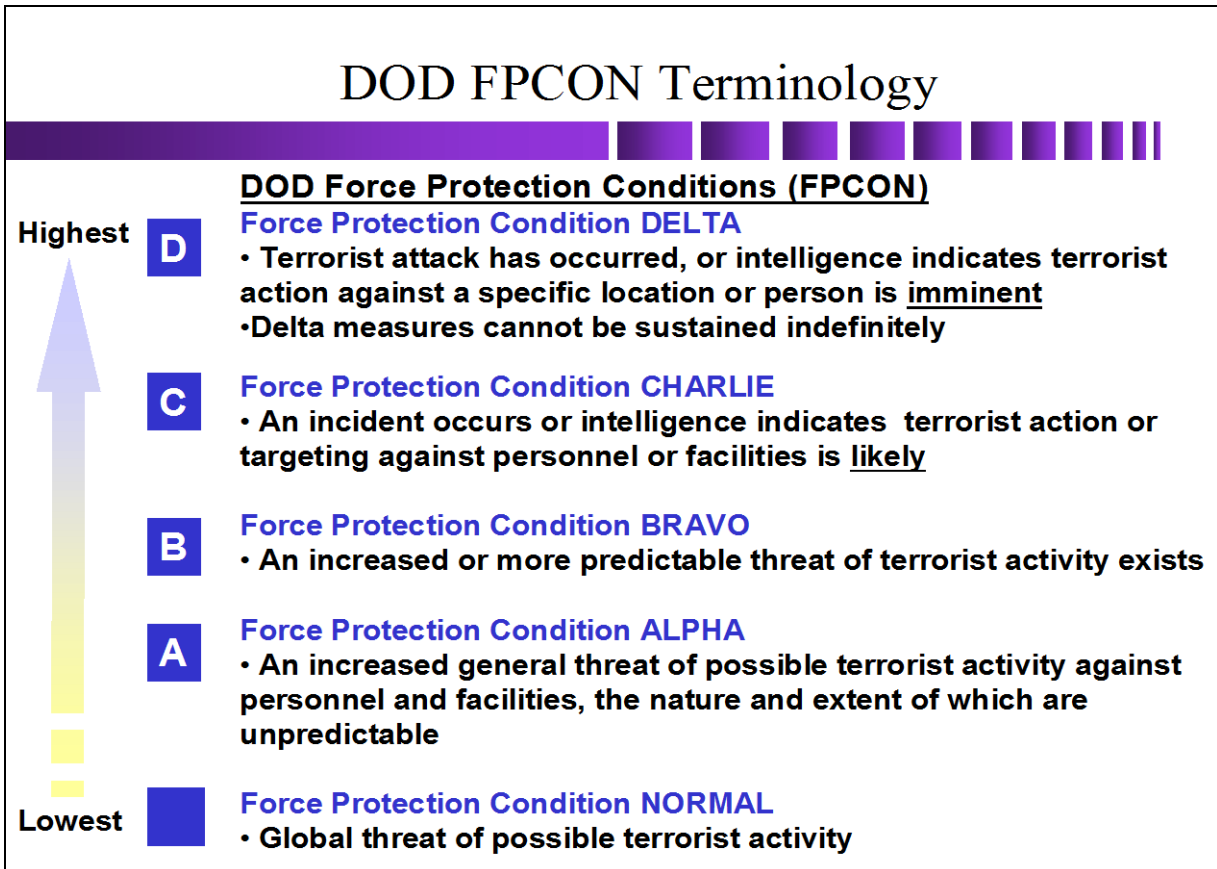


FIGURE I: Force Protection Conditions (FPCONs)

The National Terrorism Advisory System (NTAS) replaces the color-coded Homeland Security Advisory System. This new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

It recognizes that Americans all share responsibility for the nation’s security, and should always be aware of the heightened risk of terrorist attack in the United States and what they should do.

After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued.

NTAS Alerts will only be issued when credible information is available. The Secretary of Homeland Defense will announce the alerts publicly. Alerts will simultaneously be posted on the NIPRNET at <https://www.dhs.gov/national-terrorism-advisory-system> and released to the news media for distribution. The Department of Homeland Security will also distribute alerts across its social media channels, including the Department's blog, Twitter stream, Facebook page, and RSS feed.

These alerts will include a clear statement that there is an imminent threat or elevated threat. Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat. The NTAS Alerts will be based on the nature of the threat: in some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels.

NTAS Alerts contain a sunset provision indicating a specific date when the alert expires - there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

## Household Security Checklist

This generic household checklist should be used to evaluate current and prospective residences if a locally specific checklist is not available. Prospective renters should attempt to negotiate security upgrades as part of the lease contract when and where appropriate. This could reduce costs to the DoD member by amortizing costs over the period of the lease.

- Exterior Grounds:
  - If you have a fence or tight hedge, have you evaluated it as a defense against intrusion?
  - Is your fence or wall in good repair?
  - Are the gates solid and in good repair?
  - Are the gates properly locked during the day and at night?
  - Do you check regularly to see that your gates are locked?
  - Have you eliminated trees, poles, ladders, boxes, etc., that may help an intruder to scale the fence, wall, or hedge?
  - Have you removed shrubbery near your gate, garage, or front door that could conceal an intruder?
  - Do you have lights to illuminate all sides of your residence, garage area, patio, etc.?
  - Do you leave your lights on during hours of darkness?
  - Do you check regularly to see that the lights are working?
  - If you have a guard, does his/her post properly position him/her to have the best possible view of your grounds and residence?
  - Does your guard patrol your grounds during the hours of darkness?
  - Has your guard been given verbal or written instructions and does he/she understand them?
  - Do you have dogs or other pets that will sound an alarm if they spot an intruder?
  - Have you considered installation of a camera system with recording capabilities or a dummy camera system as a deterrent?
- Interior Features
  - Are your perimeter doors made of metal or solid wood?
  - Are the doorframes of good solid construction?
  - Do you have an interview grill or optical viewer in your main entrance door?
  - Do you use the interview grill or optical viewer?



- Are your perimeter doors properly secured with good heavy-duty dead bolt locks?
- Are the locks in good working order?
- Can any of your door locks be bypassed by breaking the glass or a panel of lightwood?
- Have you permanently secured all unused doors?
- Are your windows protected by solid steel bars, ornamental, or some other type of shutters?
- Are unused windows permanently closed and secured?
- Are your windows locked when they are shut?
- Are you as careful of second floor or basement windows as you are of those on the ground floor?
- Have you secured sliding glass doors and similar style windows with a broom handle, “charlie bar,” or good patio door lock?
- If your residence has a skylight, roof hatch, or roof doors, are they properly secured?
- Does your residence have an alarm system?
- Have you briefed your family and household assistants on good security procedures?
- Do you know the phone number of the police or security force that services your neighborhood?
- General
  - Are you and your family alert in your observations of persons who may have you under surveillance or who may be casing your house in preparation for a burglary or other crime?
  - Have you verified the references of your domestic help, and have you submitted their names for security checks?
  - Have you told your family and household assistants what to do if they discover an intruder breaking into or already in the house?
  - Have you restricted the number of house keys?
  - Do you know where all your house keys are?
  - Have you identified telephone contact numbers for all adults?
  - Have you identified rally points, such as at a neighbor’s house or other identified location, for use in emergencies if the house must be evacuated?

## Operations Security Guidance for Family Members

As a family member of the military community, you are a vital player in our success, and we could not do our job without your support. You also play a crucial role in ensuring your loved ones' safety just by protecting the information that you know about military day-to-day operations. Understanding critical information and identifying the methods adversaries use to collect this information is vital to the success of the Operations Security (OPSEC) program.

- **What is OPSEC?** Officially, OPSEC is a process for identifying critical information and subsequently analyzing friendly actions related to military operations and other activities to identify those actions that can be detected by adversaries or used by adversaries to discover friendly actions. In short, OPSEC is keeping potential adversaries from discovering critical DoD information, such as when units are mobilizing, where they are traveling, or what processes are involved. As the name suggests, it protects U.S. operations -- planned, in-progress, and completed. Success depends on secrecy and surprise, so the military can accomplish the mission more quickly and with less risk. Potential adversaries and even friendly nations want this information. They will not only pursue military members for the data, but they may also look to you, the family member.
- **What Can You Do?** There are many countries and organizations that would like to harm Americans and degrade U.S. influence in the world. It is possible and not unprecedented for spouses and family members of U.S. military personnel to be targeted for intelligence collection. This is true in the United States and especially true overseas! What can you do?
  - **Be Alert.** Foreign governments and organizations can collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy and, consequently, deadly to Americans. Their methods have become very sophisticated. The Internet has become the preferred method of gathering information. Family members may unwittingly provide all the necessary information to compromise the military members' mission.
  - **Be Careful.** There may be times when your spouse cannot talk about the specifics of his or her job. It is very important to conceal and protect certain information such as flight schedules, ship movements, temporary duty locations, and installation activities, just to name a few. Something as simple as a phone discussion concerning where your spouse is going on temporary duty or deploying to can be very useful to U.S. adversaries.
  - **Protect Critical Information.** Even though this information may not be classified, it is what the Department of Defense calls "critical information." Critical information deals with specific facts about military intentions, capabilities, operations, or activities. If an adversary knew this detailed information, U.S. mission accomplishment and personnel safety could be jeopardized. It must be

protected to ensure an adversary does not gain a significant advantage. By being a member of the military family, you will often know some bits of critical information. Do not discuss them outside of your immediate family and especially not over the telephone or through e-mails. Be careful of the information shared on social media, such as Facebook and Twitter.

- **Examples of Critical Information**

- Detailed information about mission of assigned units.
- Details concerning locations and times of unit deployments.
- Personnel transactions that occur in large numbers (e.g., pay information, power of attorney, wills, or deployment information).
- References to trend in unit morale or personnel problems.
- Details concerning security procedures.
- Family members' personal information.

- **Puzzle Pieces.** These bits of information may seem insignificant. However, to a trained adversary, they are small pieces of a puzzle that highlight what U.S. forces are doing and planning. Remember, the elements of security and surprise are vital to the accomplishment of U.S. goals and collective DoD personnel protection.
- Where and how you discuss this information is just as important as with whom you discuss it. Adversary's agents tasked with collecting information frequently visit some of the same stores, clubs, recreational areas, or places of worship as you do.
- Determined individuals can easily collect data from cordless and cellular phones and even baby monitors using inexpensive receivers available from local electronics stores. You are also vulnerable to data collection when connected to wireless networks.
- If anyone, especially a foreign national, persistently seeks information, notify your military sponsor immediately. He or she will notify the unit OPSEC program manager or local security office.

Members of the Armed Forces have a role in their families' security. Service members who are constantly worrying about the safety and security of family members will not be focused on their missions. It is essential that personal data that could identify family members be given essential privacy. This data includes, but is not limited to, names, pictures, phone numbers, home addresses, Defense Eligibility Enrollment Reporting System information, school/after-school activities, etc. Service members should inform family about this threat and pursue a lifestyle that ensures protection of vital family information.

## **Ground Transportation Security**

Criminal and terrorist acts against individuals usually occur outside the home and after the victim's habits have been established. Your most predictable habits involve traveling routes from home to place of duty or to commonly frequented local facilities.

### **VEHICLES OVERSEAS**

- Select a plain car wherever possible.
- Consider not using a government car that is identified as such.
- When possible, do not display decals with military or unit affiliations on your vehicle.
- Do not openly display military equipment or field gear in your vehicle.
- Maintain your automobile:
  - Keep vehicle in good repair; use trusted mechanics.
  - Always keep gas tank at least half full.
  - Ensure tires have sufficient tread.
  - Avoid leaving keys with repair shops.

### **PARKING YOUR CAR**

- Always lock your car.
- Do not leave your car on the street overnight, if possible.
- Park your car in well-lighted areas.
- Checking for suspicious persons before exiting the vehicle. If in doubt, drive away.
- Leave only the ignition key with parking attendant, not residential keys.
- Do not leave garage doors open or unlocked.
- Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage.
- Do not display decals identifying the owner as an American.
- Remove garage door opener if car is left with service or repair shop.

### **VEHICLE SECURITY**

Vehicle Inspection Tips: Every time you use your automobile, you should conduct a precautionary inspection. Make a habit of checking the vehicle and the surrounding area before entering and starting the vehicle.

- Before entering your vehicle, check the exterior for fingerprints, smudges, scratches or other signs of tampering. Ensure wheel lug nuts are tight. Examine tires for stress marks and any evidence of tampering.

- Check electronic tampering device (alarm system) if installed. An inexpensive option is to place transparent tape on the doors, hood, and trunk of your vehicle to alert you to tampering.
- Always look inside the vehicle before you move inside. Check the interior of the vehicle for things out of place. Look for suspicious or unfamiliar items.
- Consider the following steps to prevent potential vehicle tampering.
  - Always secure the doors and windows of your vehicle.
  - Let a fine coat of dust remain on the vehicle surface to help detect tampering.
  - Ensure the hood of your vehicle has a release latch located inside the vehicle.
  - Use a locking fuel cap.
  - Install an intrusion alarm.
  - Only use steel-belted radial tires for your vehicle. You may also consider the use of ‘run-flat’ tires.
- If you find something out of the ordinary, DO NOT TOUCH IT. Contact the local authorities to report your findings.

### **ON THE ROAD**

- Before leaving buildings to get into your vehicle, check the surrounding area to determine if anything of a suspicious nature exists. Display the same wariness before exiting your vehicle.
- Prior to getting into a vehicle, check beneath it for any tampering or bombs by looking for wires, tape, or anything unusual.
- If possible, vary routes to work and home.
- Avoid late-night travel when possible.
- Travel with companions.
- Avoid isolated roads or dark alleys when possible.
- Always ride with seatbelts buckled and doors locked. Keep windows closed, if possible.
- Consider carrying a cell phone in your vehicle.
- Plan your route and pre-plan alternate routes in case of emergency.
- Know the location of all emergency services along your route.
- Do not allow your vehicle to be boxed in; maintain a minimum eight-foot interval between you and the vehicle in front when stopped in traffic; avoid using curbside lanes while in heavy traffic. Where traffic laws permit, drive in the outer lane.
- Be alert while driving or riding in a vehicle.
- Know how to react if you are being followed:

- Check during turns for confirmation of surveillance.
- Do not stop or take other actions that could lead to confrontation.
- Do not drive home. If necessary, go to the nearest military base or police station.
- Mentally note the description and/or characteristics of vehicles or personnel following you.
- Report incident to military police and/or security forces.
- Recognize events that can signal the start of an attack. When one of these events occurs, start mentally preparing a course of action in case an attack develops. These events may include, but are not limited to:
  - Cyclist falling in front of your car.
  - Flagman or workman stopping your car.
  - Unusual or false police or government checkpoint.
  - Disabled vehicle and/or accident victims on the road.
  - Unusual detours.
  - An accident where your car is struck.
  - Cars or pedestrian traffic that box you in.
  - Sudden activity or gunfire.
- Know what to do if under attack in a vehicle:
  - Without subjecting yourself, passengers, or pedestrians to harm, try to draw attention to your car by sounding the horn.
  - Put another vehicle between you and your pursuer.
  - Execute immediate turn and escape; jump curbs at a 30-45 degree angle (not head on) with a maximum speed of 35 mph.
  - Ram blocking vehicle if necessary. (If you must ram a vehicle, always strike the other vehicle's tire or axle area.)
  - Go to the closest safe haven.
  - Report the incident to military police and/or security forces.

### **COMMERCIAL BUSES, TRAINS, AND TAXIS**

- Vary modes of commercial transportation.
- Select busy stops. Avoid standing in or near a group while waiting.
- Only using taxis recommended by the hotel staff. Do not always use the same taxi company.
- Do not let someone you do not know direct you to a specific cab.
- Ensure taxi is licensed and has safety equipment (seatbelts at a minimum).

- Ensure face of driver and picture on license are the same.
- Try to travel with a companion.
- If possible, specify the route you want the taxi to follow.

## Tips for Defensive Air Travel

Air travel, particularly through high-risk airports or countries, poses security problems different from those of ground transportation. Simple precautions can reduce your vulnerability to a terrorist assault.

### MAKING TRAVEL ARRANGEMENTS

- Use office symbols on orders or leave authorization if the word description denotes a high or sensitive position.
- Get an area of responsibility (AOR)-specific threat briefing from your security officer, ATO, or the appropriate counterintelligence or security organization prior to traveling. This briefing is mandatory prior to overseas travel and must occur within three months prior to travel. It should also include any AOR-specific AT requirements as directed by the geographic combatant commander. Most geographic combatant commanders put useful travel information on their Internet sites. The U.S. State Department website also contains valuable foreign travel information at <http://travel.state.gov>
- Before traveling, consult the DoD Foreign Clearance Guide (DoD 4500.54-M) to ensure you know and can meet all requirements for travel to a particular country. Also, verify applicable clearance requests have been approved for each country, read and review approval messages, and follow guidance contained therein. In addition, some geographic combatant commanders restrict travel to certain countries (this information is usually available on their public Internet sites). **The DoD Foreign Clearance Guide is For Official Use Only.** It is available on the SIPRNET at <http://www.fcg.pentagon.smil.mil>, as well as <https://www.fcg.pentagon.mil> if connected via the DoD (.mil) system. If you do not have access, check with your military organization to determine how you can obtain required information.
- Use military air, U.S. Transportation Command or Air Mobility Command military contract, or U.S. flag carriers. Avoid scheduling through high-risk areas. If necessary, use foreign flag airlines and/or indirect routings to avoid high-risk airports.
- Individual travelers should review flight itineraries generated by the Defense Travel System to ensure that connecting and continuing flights are conducted via airports that do not pose a risk of non-criminal detention or isolation to the traveler.
- When available, use government quarters or contracted hotels as opposed to privately arranged off-base hotels.

### PERSONAL IDENTIFICATION

- Do not discuss your military affiliation, job titles, or responsibilities with strangers.
- Consider using a tourist passport if you have one with the necessary visas, provided the country you are visiting allows it.



- If you carry your official passport, military ID, travel orders, and related documents, select a hiding place onboard the aircraft to “ditch” them in case of a hijacking. (The inner part of the window may be a quick and effective place.)
- Do not carry classified documents unless they are absolutely mission essential. E-mail documents ahead whenever possible or use alternate shipment means.

### **LUGGAGE**

- Use plain, civilian luggage; avoid military-looking bags, B-4 bags, duffel bags, etc.
- Remove all military patches, logos, or decals from your luggage and briefcase.
- Ensure luggage tags do not show your rank or military address.
- Do not carry official papers in your briefcase. If official papers must be carried, place them in a sealed, non-descript folder in your briefcase.

### **CLOTHING**

- Travel in conservative civilian clothing when using commercial transportation or military airlift if you are to connect with a flight at a commercial terminal in a high-risk area. Some geographic combatant commanders, including U.S. European Command (USEUCOM), have imposed restrictions on the wearing of military uniforms aboard commercial aircraft or vessels within their respective AOR. Check requirements before traveling.
- Do not wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.
- Do not wear U.S. identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.
- Wear a long-sleeved shirt if you have visible U.S.-affiliated tattoos.
- Do not get a fresh, close military haircut before going on international trips.

### **PRECAUTIONS AT THE AIRPORT**

- Arrive early and watch for suspicious activity.
- Look for nervous passengers who maintain eye contact with others from a distance.
- Observe what people are carrying. Note behavior not consistent with that of others in the area.
- No matter where you are in the terminal, identify objects suitable for cover in the event of attack. Pillars, trash cans, luggage, large planters, counters, and furniture can provide protection.
- Do not linger near open public areas. Proceed through security checkpoints as soon as possible in order to be in a more secure area.
- Avoid secluded areas that provide concealment for attackers.
- Be aware of unattended baggage anywhere in the terminal.

- Be extremely observant of personal carry-on luggage. Thefts of briefcases designed for laptop computers are increasing at airports worldwide. Likewise, luggage not properly guarded provides an opportunity for a terrorist to place an unwanted object or device in your carry-on bag. As much as possible, do not pack anything you cannot afford to lose; if the documents are important, make a copy and carry the copy.
- Observe the baggage claim area from a distance and claim your luggage at first opportunity, without forcing your way through large crowds. Proceed to the customs lines at the edge of the crowd.
- Report suspicious activity to the airport security personnel.

#### **ACTIONS IF ATTACKED IN AN AIRPORT**

- Dive for cover. Do not run. If you must move, crawl, and stay low to the ground, using available cover. If the threat is from weapons fire, avoid lying on floors or standing along walls as ricocheting bullets and projectiles tend to “hug” floors and walls.
- If you see grenades, seek immediate cover; lay flat on the floor, feet and knees tightly together, with soles toward the grenade. In this position, your shoes, feet, and legs protect the rest of your body. Shrapnel will rise in a cone from the point of detonation, passing over your body.
- Place arms and elbows next to your ribcage to protect your lungs, heart, and chest. Cover your ears and head with your hands to protect neck, arteries, ears, and skull.
- Responding security personnel will not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lie still until told to get up.

#### **ACTIONS IF HIJACKED**

- Determining the best response in a hostage situation is a critical judgment call. Passengers need to remain extremely alert and rational to try to understand the intentions of the hijackers. Sitting quietly may be prudent in most circumstances, but it is conceivable the situation may require actions to not allow hijackers to take control of the aircraft. In all situations, it is important for individuals to remain alert to unexpected events, think clearly, and act responsibly.
- Remain calm; be polite and comply with the physical/verbal instructions provided by your captors.
- Be aware that not all hijackers may reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by other hijackers.
- Surrender your tourist passport in response to a general demand for identification.
- Do not offer any information; confirm your military status only if directly confronted with the fact. Be prepared to explain that you always travel on your personal passport and that no deceit was intended.
- Discreetly dispose of any military or U.S.-affiliated documents.

- Do not draw attention to yourself with sudden body movements, verbal remarks, or hostile looks.
- Prepare yourself for possible verbal and physical abuse and deprivation of food, drink, and sanitary conditions.
- Discreetly observe your captors and memorize their physical descriptions. Include voice patterns and language distinctions, as well as clothing and unique physical characteristics. Observe how they are armed.
- If possible, observe if the pilots remain in control of the aircraft.
- Be aware that there could be federal authorities, such as Air Marshals, on the aircraft who may be better suited to take action.
- If an Air Marshal or flight attendant requests your assistance while taking action, help them as best you can.
- During rescue attempts, stay low in a seated, or “crash” position, until told to rise and cooperate with all instructions from the rescuers.

## **Tips for Active Shooter Response**

Active shooters are individuals who attempt to injure or kill people in confined and populated areas, often displaying no pattern in their selection of victims. Active shooter situations tend to be unpredictable and evolve quickly, often before law enforcement personnel arrive. To increase you and your family's chance of survival in an active shooter situation, you should familiarize yourself with the following information.

### **INDICATORS OF A POTENTIALLY VIOLENT BEHAVIOR**

Early recognition of a threat can prevent an incident. The following are indicators of potentially violent behavior:

- Aggression or threats towards coworkers.
- Presence of unauthorized weapons.
- Abnormal mood swings or depression, withdrawn behavior, decrease in hygiene, paranoia (i.e. "everyone is against me"), increased use of alcohol or illegal drugs.
- Suicidal remarks or comments about "putting things in order."
- Repeated violations of policies, regulations, or laws.
- Talk of severe financial problems.

History indicates that individuals that have become active shooters in a workplace display potentially violent behavior over time. If you recognize these behaviors, inform your supervisor. If you perceive an immediate threat, alert unit security.

### **EVACUATE**

You need to quickly determine the most reasonable way to protect your life, as well as those around you, whenever possible. If you can escape, consider the following:

- Have an escape route and plan in mind.
- Evacuate regardless of whether others agree to follow.
- Leave your belongings behind.
- Help others escape, if possible.
- Prevent individuals from entering an area where the active shooter may be.
- Keep your hands visible.
- Follow the instructions of security personnel.
- Do not attempt to move wounded people.
- Call emergency personnel when you are safe.

### **SHELTER IN PLACE**

If evacuation is not possible, find a place where the active shooter is less likely to find you. The place you choose should:

- Be out of the active shooter's view.
- Provide protection if shots are fired in your direction (i.e. an office with a closed and locked door).
- Not trap you or restrict your options for movement.
- Have furniture to block the door, if possible.

Lock the door, silence your cell phone, hide behind large items, remain quiet and calm, and call emergency personnel. If you are not able to speak, leave the line open to allow the dispatcher to listen.

If you are attacked, you can adapt your response to the type of weapon being used by an attacker:

- Ricocheting bullets tend to hug the floor; crouching (not lying) on the floor may reduce exposure.
- Grenade shrapnel rises from the detonation location; lying on the floor reduces exposure and having feet toward the blast may protect your head.

### **TAKE ACTION AGAINST THE ACTIVE SHOOTER**

As a last resort, and only when your life is in imminent danger, try to disrupt or incapacitate the shooter by:

- Acting aggressively against him or her.
- Throwing items and improvising weapons.
- Yelling.

Taking action against the active shooter is extremely risky, but it may be the best chance of survival for you and others. If you decide to assume the risk, you must remain committed to your actions. Time actions to coincide with the shooter's need to remove/replace magazine; respond with speed, stealth, and violence of action.

### **COOPERATE WITH FIRST RESPONDERS**

When first responders arrive, support their efforts and do not be a distraction:

- Remain calm and follow instructions.
- Put down any items in your hands.
- Raise hands and spread your fingers.
- Avoid quick movements.
- Do not cling to emergency personnel.
- Avoid pointing, screaming, or yelling.
- Do not stop to ask first responders for help or direction when evacuating.
- Evacuate in the direction first responders are entering.

- After being rescued, individuals may be initially restrained, searched, and treated as suspects.

First responders will need the following information:

- Location of the active shooter.
- Number of shooters.
- Physical description of shooter(s).
- Number and type of weapons held by the shooter(s).
- Number of potential victims.

## **Responding to Chemical Threats**

### **GENERAL INFORMATION**

Chemical agents are generally liquids, often aerosolized. Although some effects are delayed, most induce an immediate response. There are many different potential chemical warfare agents, toxic industrial chemicals, and toxic industrial materials that a terrorist could use as a weapon. Nonetheless, the following broad generalizations can be made:

- Although food or water contamination is possible, inhalation is the most likely method of contact. Protection of the breathing airway is the single most important factor of defense.
- Generally, chemical agents tend to present an immediate noticeable effect. Medical attention should be sought immediately even if exposure is thought to be limited.
- Most chemical agents that present an inhalation hazard will break down fairly rapidly when exposed to sun, diluted with water, or dissipated in high winds.
- No matter what the agent or particular concentration, evacuation (preferably upwind from the area of attack) is always advisable even if you are equipped with an appropriate breathing device and protective clothing.
- If inside a building with contamination outside, remain inside and shelter in place.

### **DETECTION**

A chemical attack or incident will not always be immediately apparent because many agents are odorless and colorless. Be alert to the possible presence of an agent. Indicators of such an attack include:

- Droplets of oily film on surfaces.
- Unusual dead or dying animals in the area.
- Unusual liquid sprays or vapors.
- Unexplained odors (smell of bitter almonds, peach kernels, newly mowed hay, or green grass).
- Unusual or unauthorized spraying in the area.
- Low-lying clouds of fog unrelated to weather; clouds of dust; or suspended, possibly colored, particles.
- People dressed unusually (long-sleeved shirts or overcoats in the summertime) or wearing breathing protection, particularly in areas where large numbers of people tend to congregate, such as subways or stadiums.
- Victims displaying symptoms of nausea, difficulty breathing, convulsions, disorientation, or patterns of illness inconsistent with natural disease.

## DEFENSE IN CASE OF CHEMICAL ATTACK

Protection of airways is the single most important thing a person can do in the event of a chemical attack. In most cases, absent a gas mask, the only sure way to protect an airway is to put distance between you and the source of the agent. While evacuating the area, cover your mouth and nose with a handkerchief, coat sleeve, or any piece of cloth to provide some moderate means of protection. Other steps are:

- Move upwind from the source of attack.
- If evacuation from the immediate area is impossible, move outdoors or to an interior room on a higher floor. Remember many agents are heavier than air and will tend to stay close to the ground.
- If indoors and no escape outside is possible, close all windows and exterior doors while also shutting down the air conditioning or heating systems to prevent circulation of air. Notify responders as soon as possible of your location.
- Cover your mouth and nose. If gas masks are not available, use a surgical mask or handkerchief. An improvised mask can be made by soaking a clean cloth in a solution of one tablespoon of baking soda in a cup of water. Although not highly effective, it may provide some protection.
- Cover exposed extremities and make sure any cuts or abrasions are covered and bandaged.
- If splashed with an agent, immediately wipe it off using generous amounts of warm soapy water or a diluted 10:1 bleach solution.
- If water is not available, talcum powder or flour are also excellent means of absorbing liquid agents. Sprinkle the flour or powder liberally over the affected skin area, wait 30 seconds, and gently wipe off with a rag or gauze pad.
- No matter the agent or concentration, medical attention should be sought immediately, even if the exposure is thought to be limited.



# Responding to Biological Threats

## GENERAL INFORMATION

Biological agents are organisms or toxins that have the ability to kill or incapacitate people, livestock, and crops. Three basic groups of biological agents that could be used as weapons are bacteria, viruses, and toxins. Most biological agents break down quickly when exposed to sunlight, although others, such as anthrax, can live much longer. The following are potential delivery methods for biological attacks:

- Aerosols -- biological agents are dispersed into the air, forming a fine mist that may drift for several miles.
- Animals -- some diseases are spread by insects and animals.
- Food and water contamination -- some pathogenic organisms and toxins may persist in food and water supplies. Most microbes can be killed, and toxins deactivated, by cooking food and boiling water. Follow official instructions.
- Person-to-person -- spread of a few infectious agents is also possible. Humans, for example, have been the source of infection for smallpox and plague.

## DETECTION

Public officials may not immediately be able to provide information on what you should do. It will take time to determine what the illness is, how it should be treated, and who is in danger. Watch television, listen to radio, or check the Internet for official news and information, including signs and symptoms of the disease, areas in danger, if medications or vaccinations are being distributed, and where you should seek medical attention if you become ill.

The first evidence of an attack may be when you notice symptoms of the disease caused by exposure to an agent. Be suspicious of any symptoms you notice, but do not assume that any illness is a result of the attack.

## DEFENSE IN CASE OF BIOLOGICAL ATTACK

If you become aware of an unusual and suspicious substance nearby:

- Move away quickly.
- Wash with soap and water.
- Contact authorities.
- Listen to the media for official instructions.
- Seek medical attention if you become sick.
- Turn off HVAC systems.

If you are exposed to a biological agent:

- Remove and bag your clothes and personal items. Follow official instructions for disposal of contaminated items.
- Wash yourself with soap and water and put on clean clothes.
- Seek medical assistance. You may be advised to stay away from others or even quarantined.

# Responding to Radiological Threats

## GENERAL INFORMATION

Terrorist use of a radiological dispersion device (RDD), or “dirty bomb,” is considered far more likely than the use of a nuclear explosive device. An RDD combines a bomb with radioactive material in order to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Radioactive materials in RDDs are widely used in medicine, agriculture, industry, and research, and are easier to obtain than weapons-grade uranium or plutonium.

The size of the affected area and the level of destruction caused by an RDD would depend on the sophistication and size of the conventional bomb, the type of radioactive material used, the quality and quantity of the radioactive material, and the local meteorological conditions -- primarily wind and precipitation. The affected area would likely be off limits for an extended period of time.

## DETECTION

Although the explosive blast will be immediately obvious, the presence of radiation will not be known until trained personnel with specialized equipment are on the scene. It would be safer to assume radiological contamination has occurred -- particularly in an urban setting or near other likely terrorist targets -- and take the proper precautions.

## DEFENSE IN CASE OF RDD ATTACK

If the explosion or radiological release occurs inside, get out immediately and seek safe shelter.

If the release occurs outside, and you are outdoors:

- Seek shelter indoors immediately in the nearest undamaged building.
- Cover your mouth and nose, as well as any exposed extremities.
- If appropriate shelter is not available, move as rapidly as is safe upwind and away from the location of the explosive blast. Then seek appropriate shelter as soon as possible.
- Listen for official instructions and follow directions.

If the release occurs outside, and you are indoors:

- Seek shelter immediately, preferably underground or in an interior room of a building, placing as much distance and dense shielding as possible between you and the outdoors where the radioactive material may be.
- If you have time, turn off ventilation and heating systems, close windows, vents, fireplace dampers, exhaust fans, and clothes dryer vents. Retrieve your disaster supplies kit and a battery-powered radio and take them to your shelter room.

- Seal windows and external doors that do not fit snugly with duct tape to reduce infiltration of radioactive particles. Plastic sheeting will not provide shielding from radioactivity or from blast effects of a nearby explosion.
- Listen for official instructions and follow directions.

After finding safe shelter, those who may have been exposed to radioactive material should decontaminate themselves. To do this, remove and bag your clothing (and isolate the bag away from you and others) and shower thoroughly with soap and water. Seek medical attention after officials indicate it is safe to leave shelter.

Follow these additional guidelines after an RDD event:

- Continue listening to your radio or watch the television for instructions from local officials, whether you have evacuated or sheltered-in-place.
- Do not return to or visit an RDD incident location for any reason.

**Section II**

---

---

**Guidance for Isolated Personnel****POLICY**

Preserving the lives and well-being of U.S. military, DoD civilians, and DoD contractor personnel authorized to accompany the U.S. Armed Forces who are in danger of becoming, or already are, beleaguered, besieged, captured, detained, interned, or otherwise missing or evading capture (hereafter referred to as “isolated”) while participating in U.S.-sponsored activities or missions, is one of the highest priorities of the Department of Defense. The United States Government (USG) and its allies will use every appropriate resource to gain the safe return of isolated personnel, those detained by foreign governments, or taken hostage<sup>1</sup> by insurgents, criminal gangs, or terrorist groups. It is USG policy to deny hostage-takers the benefits of ransom, prisoner releases, policy changes, or other acts of concession. However, the USG and allied governments may enter into a dialogue with representatives of those holding hostages in order to ensure the safe return of all isolated personnel.<sup>2</sup>

**SCOPE**

Military personnel should follow guidance from the Code of Conduct. The Code of Conduct is a moral guide designed to assist military personnel in combat or being held as prisoners of war to live up to the ideals contained in the DoD policy. DoD civilians, DoD contractors (under the terms of the contract), family members, and other designated personnel should know their personal legal status under the Geneva Conventions. Knowledge of their personal legal status shall assist those who become captured or isolated to apply properly the rights and privileges afforded to them under international law. More information concerning individual legal status can be gained from the command legal advisor or ATO.

**A. Conduct of Isolated Personnel**

Personnel should consistently conduct themselves in a manner that avoids discrediting themselves and their country and have faith in themselves, their comrades, and country. Isolated personnel should be proactive and maintain a positive attitude that recovery forces are doing everything they can to locate and recover them. Personnel should do everything possible to return to friendly control, assist other Americans and their allies with whom they are isolated, and do nothing that may harm a fellow American or ally. They should resist, to the utmost of their ability, captor exploitation and protect classified and sensitive information at all times. They should not accept special treatment from a captor, unless such treatment is unconditional. Attempt to extend any unconditional treatment to all Americans and allies in the same situation. To their best ability,

---

<sup>1</sup> (U) For common understanding, the term *hostage* throughout this document denotes captivity by non-government entities (e.g., terrorist groups, rebels, criminals, insurgents, and militia).

<sup>2</sup> (U) U.S. Department of State (DOS) Foreign Affairs Manual Volume 7: Hostage Taking and Kidnapping, “The US will use every appropriate resource to gain the safe return of US citizens who are held hostage.” 27 April 11, <http://www.state.gov/documents/organization/86829.pdf>

personnel should make no written, oral, or videotaped statements harmful to the U.S. or its allies.

### **RATIONALE**

Because of their wide range of foreign travel, DoD personnel participate in activities that can result in detention or captivity state and non-state actors. The guidance in this section seeks to help DoD personnel survive these situations with honor and does not constitute a means for judgment or replace the Uniform Code of Military Justice or other applicable law as a vehicle for enforcement of proper conduct. This guidance, although exactly the same as the Code of Conduct in some areas, applies only during operations or situations not related specifically in the Code, such as terrorist captivity.

### **GENERAL**

DoD personnel (and their family members) captured by terrorists or detained by hostile foreign governments are often held for individual exploitation, to influence the USG, or both. This exploitation can take many forms, but each form of exploitation is designed to assist the foreign government or the terrorist captors. In the past, terrorists or governments exploited detainees for information and propaganda efforts, including confessions to crimes never committed. This assisted or lent credibility to the detainer. Governments also have been exploited in such a situation to make damaging statements about themselves or to force them to appear weak in relation to other governments. Governments have paid ransoms for captives of terrorists and such payments have improved terrorist finances, supplies, status, and operations, often prolonging the terror carried on by such groups. The USG policy is that it will not negotiate with terrorists.

### **RESPONSIBILITY**

The USG will make every good-faith effort to obtain the earliest release of DoD personnel (and their family members), whether detainees or hostages. Faith in one's country and its way of life, faith in fellow detainees or captives, and faith in one's self are critical to surviving with honor and resisting exploitation. Resisting exploitation and having faith in these areas are the responsibility of all Americans. On the other hand, the destruction of such faith must be the assumed goal of all captors determined to maximize their gains from a detention or hostage situation.

### **GOAL**

DoD personnel must take every reasonable step to prevent exploitation of themselves and the USG. If the captive cannot prevent exploitation completely, the captive must take every step to limit exploitation as much as possible. Detained DoD personnel often are catalysts for their own release, based on their ability to become unattractive sources of exploitation; e.g., one who resists successfully may expect detainers to lose interest in further exploitation attempts. Detainees or hostages must make their own judgments as to how their actions will increase their chances of returning home with honor and dignity. Without exception, the military member who may say honestly that he or she has done his or her utmost in a detention or hostage situation to resist exploitation upholds DoD policy, the founding principles of the United States, and the highest traditions of military service.

## **MILITARY BEARING AND COURTESY**

U.S. military personnel will maintain their military bearing, regardless of the type of detention or captivity or harshness of treatment. They should make every effort to remain calm, courteous, and project personal dignity. That is particularly important during the process of capture and the early stages of internment when the captors may be uncertain of their control over the captives. Discourteous, nonmilitary behavior seldom serves the long-term interest of a detainee or hostage and often results in unnecessary punishment that serves no useful purpose. In some situations, such behavior may jeopardize survival and severely complicate efforts to gain release of the detainee or hostage.

## **CLASSIFIED INFORMATION**

There are no circumstances in which a detainee or hostage should voluntarily give classified information or materials to those unauthorized to receive them. To the utmost of their ability, DoD personnel held as detainees or hostages will protect all classified information. An unauthorized disclosure of classified information, for whatever reason, does not justify further disclosures. Detainees and hostages must resist, to the utmost of their ability, each and every attempt by their captor to obtain such information.

## **MILITARY CHAIN OF COMMAND**

In group detention, captivity, or hostage situations, military detainees or hostages will organize, to the fullest extent possible, in a military manner under the senior military member present and eligible to command. The importance of such organization cannot be overemphasized. Historically, in both peacetime and wartime, establishment of a military chain of command has been a tremendous source of strength for all captives. Every effort will be made to establish and sustain communications with other detainees or hostages. Military detainees or hostages will encourage civilians being held with them to participate in the military organization and accept the authority of the senior military member. In some circumstances, such as embassy duty, military members may be under the direction of a senior U.S. civilian official. Notwithstanding such circumstances, the senior military member still is obligated to establish, as an entity, a military organization and to ensure that the guidelines in support of the DoD policy to survive with honor are not compromised.

## Pre-Mission Isolation Planning

### How to prepare for isolation:

- Follow all local force protection guidance to avoid hazardous situations.
- Develop a plan to communicate, flee, and fight, if necessary. Holding out for a short span of time may make the difference in being taken captive or not.
- Develop a plan of action with several backup plans before departing a secure area.
- Be familiar with the route and map -- study it in detail.
- Ensure vehicles are reliable and have all necessary emergency equipment.
- Study the local norms and be alert to situations and changes in behaviors of the locals that may signal that something bad is about to happen -- clear the area.
- Have a “grab and go” kit. It should include a communications device (cell phone or radio), water, basic first aid kit, etc. Consider including local clothing to assist in any necessary improvised disguise. A weapon with extra ammunition may be appropriate if local conditions permit lawful possession.
- Have personal affairs in order, and prepare family members for the potential of isolation.
- Develop the will to survive and resist. Mental preparation is invaluable, and demonstrating a strong will can help overcome seemingly overwhelming obstacles.

In addition, in expeditionary locations, work with local military officials to:

- Develop an emergency communications plan that provides connectivity to military or governmental support units. Include potential emergency contact ground-to-air signals (GTAS). Ensure all personnel know how to implement the plan.
- Maintain situational awareness -- blocked streets or someone trying to direct traffic down a side street could be a funneling effort for an ambush or toward an improvised explosive device.

**Factors for Successful Evasion and Recovery.** Pre-mission area study and attention to detail are essential for successful evasion and recovery. **NOTE:** This document uses the term Evasion Plan of Action (EPA) when discussing developing and documenting generic and specific evasion planning regardless if an individual is documenting an EPA, PR action plan, or a similar type document. When developing evasion plans, individuals should become familiar with any theater specific PR planning documents available to them. Individuals should also become familiar with available recovery resources within the region, including regional and allied nation capabilities. A thorough study of maps and imagery will assist in preparing an evasion plan.

**Evasion Plan of Action.** Having an EPA is essential to personnel subject to isolation in high threat areas regardless of the U.S. or allied military presence. It provides details allowing theater personnel recovery managers to focus employment of nearby or available recovery forces. The EPA tells searchers where to look and what to look for. Personnel should develop EPAs with certain goals in mind: understanding the threat, developing appropriate plans, and clearly articulating the actions a person intends to take



should isolation occur. First, personnel should face the reality they may become isolated. Having knowledge of the threats in the operating area will help people understand the risk involved. Secondly, personnel can develop an EPA designed to keep them alive, free, and determine several courses of action that may contribute to their return to friendly control. It will also assist individuals in preparing for and gaining situational awareness during an isolation event. Third, personnel should document their plans in an EPA to assist recovery forces in understanding their intentions should isolation occur. Individuals should follow the EPA when possible, but modify plans if required when faced with on-the-ground realities. Even if not usable, the EPA provides a framework for organized thought when needed most.

**Equipment Preparation.** All personnel should check their equipment. Pre-loading cell phones with emergency contact, speed-dial phone numbers, including those of the closest Joint Personnel Recovery Center, Personnel Recovery Coordination Cell, and the U.S. or allied embassies may be beneficial. Personnel should avoid pre-loading any personal numbers. Personnel should test all battery-powered equipment and read the battery meters to ensure ample power is available. Personnel should always bring at least one change of batteries for each piece of battery-powered equipment. Reduce the risk of equipment malfunction by taking precautions to protect equipment from environmental extremes, grit, and moisture. Personnel should ensure to pack fragile equipment, including water containers, in a manner that will protect them from physical damage that would render the device unusable (protect easily punctured water/equipment containers from thorns, jagged rocks, and exposed metal). It is critical for personnel to be proficient at operating their equipment under all conditions as limited time and adverse conditions will challenge isolated personnel trying to securely report their position and situation. Learning how to operate equipment during isolation is not an ideal situation.

**Personal Survival Kits.** Creating and carrying a personal survival kit will augment any issued survival equipment in order to help an isolated person survive. Individuals must personalize their survival kits for the operating environment. Consider including the following items in a personal survival kit: water, shade tarp, ammunition, radio, personal locator beacon (PLB), satellite phone, commercial tracking device, maps, compass, and emergency signaling devices, local purchase cell phone, sun block, insect repellent, head net, space blanket, burlap, poncho, a mirror, infrared (IR) and visible lights (e.g.: Fire Flies, laser pointer, Micro Lights, Phoenix, chemical lights, etc.), 3'x3' bright colored cloth, 1 sq. inch of glint tape, knife or multi-tool, fire starter, candle, button compass, water purification tablets, three 1-gallon zip lock bags, large plastic leaf/trash bag (for water storage and protection from the elements), 100 ft. parachute cord, gloves, large needles, dental floss, safety pins, first aid items, and any needed medications. If extra clothing is included, it should be lightweight, windproof, waterproof, and appropriate for cultural, environmental, and seasonal conditions. An outer jacket and hat and sturdy local footwear could be useful for blending with the local population. Having a small or moderate amount of local and U.S. currency may be useful for purchasing supplies or materials. During pre-mission planning, personnel should consider the different survival situations when deciding what to pack in their personal survival kits. Personnel should

also determine which items are necessary to retain in an emergency and which are expendable.

**Vehicle Survival Kits.** If using a vehicle, maintenance is essential. Personnel should anticipate possible mechanical problems and prepare to minimize the effects. Check vehicles regularly; urban (broken glass, nails, concrete) or rural debris (thorns and jagged rocks) may puncture tires. Personnel should make certain the vehicle's spare tire is in good working order. Vehicles should be prepared with survival kits including extra water, mechanical water filtration device, camouflage tarp or netting, spare fluids, belts, and filters, basic tools, emergency repair kit (duct tape, wire, parachute cord, and emergency adhesive), tow chain or strap, ax, machete, and shovel. If traveling off road, personnel should prepare and carry equipment to extract the vehicle from vegetation, soft sand, or mud. Include items that could serve as shelter materials (blankets, tarps). Personnel should include a bucket, rope, and gloves as part of the vehicle survival kit.

**Communication Plans.** The number one priority for an isolated person is to contact friendly authorities to report their identity and location by using the established communications plan. Document the communication plan on the EPA. Communication plans should address both short-term and long-term communication with friendly forces. The plan should include radio, phone (cell or satellite) information, contact times, frequencies, and intentions.

**Personal Force Protection Measures.** Personnel should accomplish pre-mission force protection planning to help prevent isolation. To avoid or lessen the chance of isolation, personnel must practice common sense protective measures. *Traveling alone anywhere, especially in an area with potential for violent conflict with armed groups or criminals is not recommended.* Personnel should not leave cash or other valuables unsecured or wear expensive jewelry or show large amounts of cash. Personnel should maintain a low profile; do not display items of value (i.e. Smart phones, laptops, iPods, cameras); dress in styles similar to the local population if appropriate and refrain from using a cell phone on the street. Personnel should inform supervisors and co-workers of destinations and anticipated arrival and departure times.

## Recovery

**Signaling for Recovery.** Timely and effective signaling will greatly help efforts to report, locate, identify, support, and recover isolated personnel. The best location information comes from the individual who is equipped with a survival radio, cell phone, or other communication device and trained to report their current position. The isolated person's participation in providing their location to recovery forces is by far the most accurate, efficient, and expedient means of locating their position for recovery. Another good source for determining location is if recovery forces locate a radio's signal or detect a visual signal. Recovery forces will look at the isolated person's EPA to determine their signaling intentions. Based on the information in the EPA, recovery forces can search areas and potentially authenticate the identity of the isolated person.

**Technical Communication.** Personnel should document their EPA with detailed information on available communication device(s) to include make, model, frequency, serial number, SIM card data, international mobile equipment identity (IMEI) or electronic serial numbers (ESNs).<sup>3</sup> Personnel should attempt to contact friendly authorities by transmitting a distress call via any available communication device. Isolated personnel should be prepared to identify themselves, authenticate, and transmit their location when directed. Besides requiring batteries, there are other potential issues when relying on radios or cell phones. Radios or cell phones may malfunction, sustain damage, become lost/stolen, or lose their programming/power. Cell phones have an additional connectivity concern in that they may be unable to obtain a cell tower's signal or are incompatible with a country's communication system. Personnel should anticipate these problems and prepare to overcome them.

**Personal Locator Beacons (PLBs).** PLBs are a family of hand-held devices that transmit distress signals on an internationally monitored frequency. PLBs are not the primary means for alerting recovery forces during an isolating event. Personnel should follow the communications plan, as annotated in their EPA, to determine the appropriate time to activate a PLB. If necessary, personnel should use PLBs to report their situation when other prescribed methods are not available or are not working. Personnel should only use a PLB when all other means of reporting are unavailable, exhausted, or ineffective. They only broadcast distress and homing signals. Personnel should annotate their PLB's unique identifier number in their EPA or other similar emergency action plan. This will greatly assist alerted recovery personnel in confirming whether a transmission is an actual report of an isolation event or an inadvertent alarm. When employing a PLB, the greatest probability of successful satellite reception occurs when a PLB has a clear view of the sky from horizon-to-horizon. They are capable of operating in an environment with less than a complete view of both horizons (e.g., a valley, canyon, on a mountainside, wooded area, near a chain link fence, nearby or inside buildings), but

---

<sup>3</sup> (U) Depending on the type, age, capability, and manufacturer, cellular service providers can identify when a specific mobile phone is active on a particular mobile network by using an ESN, mobile equipment identifier or IMEI. Personnel can find these codes by following instructions available in their phone User Guides or on the service provider's website under Support. At a minimum, personnel can find their phone's IMEI by dialing \*#06# into the handset.

any such obstruction will reduce satellite reception capability and/or degrade the PLB's signal; however, even if reception is clear, some signal information may be delayed and take up to an hour and a half before it gets to the to the appropriate agency which can respond to an activation.

**Visual Signals.** Isolated personnel may find themselves in a nontechnical communication situation due to drained batteries, loss, damage, or confiscation of their radio. PR plans should include alternate procedures for signaling when radio contact fails, is not feasible, or is not available.

**Ground-to-Air Signals (GTAS).** A GTAS is a supplemental system to radio or cell phone communications. They are non-directional signals that identify an individual's general location. Signal construction could consist of colored (parachute) panels, specially aligned radar reflective devices, glint tape, specially shaped IR reflectors, metallic trash (cans, foil, sheet metal, screen wire, vehicle parts), building debris, natural materials (e.g., sticks, logs, rocks, sod, dug or turned soil, vegetation), to make a visually recognizable or meaningful signal. Individuals should annotate the EPA with the type of signal they intend to use and the distance and direction they intend to travel in relation to all visual signals. Personnel should choose materials appropriate to the environment and those that will not degrade in weather. Isolated personnel may signal the approaching recovery asset by using a directional signal aimed towards the recovery asset to pinpoint the individual's specific location. Directional signals include mirrors, flashlights, laser lights, shielded IR lights, chem-lights and specially shaped IR reflectors. If isolated in a hostile environment, and in voice contact with a recovery force, personnel should employ non-directional signals, such as flares and smoke, only when directed. Isolated personnel may need to improvise signaling devices (car or bike mirror, polished metal, bright colored cloth, etc.) and become very creative to avoid enemy detection.

**Recovery.** Availability of potential U.S., allied or regional recovery assets are dependent on the situation at the time of isolation; time, threats, and distance are limiting factors. Because of the long distances and lack of traditional recovery assets, it may take a significant amount of time to execute a recovery mission. Personnel should plan to survive and evade unassisted for a minimum of 72-96 hours. However, recovery may take longer. Isolated personnel must also be prepared for long-term unassisted evasion. If isolation occurs in a neighboring country, diplomatic clearance may be required before allied forces can conduct their own operations to recover personnel. Despite a lack of traditional recovery capability, isolated personnel can be sure U.S. and allied forces will make every effort to effect their recovery.

## Captivity

All captives have a legal and moral obligation to resist the enemy and support fellow isolated personnel to do the same. Maintaining communications is one of the most important ways for captives to aid one another. Communication breaks down the barriers of isolation that a captor may attempt to construct and helps strengthen an individual's will to resist. Immediately upon capture, each person should try to make contact with fellow captives by any means available, continue to communicate, and vigorously participate as part of the organization. Isolated personnel must be proactive and maintain a positive attitude that recovery forces are working to locate and recover them, resist exploitation, and keep faith that the U.S. and allied governments will do everything in their power to get them home. Captives must make their own judgments as to which actions will increase their chances of returning home with honor.

**General Captor Behavior.** While governmental detentions are generally a predictable captivity situation, hostage detention is at the opposite end of the spectrum and is generally the least predictable and least structured form of captivity. Foreign government forces should demonstrate constrained behavior towards detained U.S. and allied personnel due to international influence and the desire to maintain good relations with the U.S. and its allies. Further, if allied or regional governments detain U.S. or allied personnel, personnel can expect resolution of their situation through diplomatic intervention. Conversely, in hostage-taking incidents, the captors may not feel constrained in their treatment towards their prisoners. Hostage-takers may likely be nervous and unsure, easily irritated, and often irrational. Additionally, hostage-takers seldom feel bound or obligated to the guidelines delineated in International Humanitarian Law. As a result, hostages have lost their lives while held by non-governmental captors around the world. The possible types of seizure vary from spontaneous "target of opportunity" hostage taking, to carefully planned and well-orchestrated abductions. If isolated personnel are uncertain whether captors are government detainers, criminals, or terrorists, they should assume they are the latter until proven otherwise.

**Value of Captives.** U.S. and allied personnel held captive in the region are valuable to any governmental, criminal, or terrorist organization. Captor groups will likely transport U.S. personnel away from the initial capture point to a safe holding area and exploit them for intelligence, political, or propaganda purposes. Criminals will attempt to extort large sums of money from governments, corporations, families, or even sell the hostage to another group or government. However, a hostage's value may not prevent hostage-takers from physically harming or killing the hostage if they become a liability. Captives will need to apply situational awareness to assess what their perceived value is in the eyes of the captor and captor intentions. In some cases, it may be necessary to lower the captors' expectations of a large ransom. The captive should continuously try to convince the captor that they are more valuable alive than dead.

**Surviving the Initial Stage of Captivity.** Situational awareness, observation, and focusing on the captor's behavior and intentions are very important. If captured, isolated

personnel should try to determine the identity or affiliation of the captor group and assess the immediate security situation. If the individual believes immediate escape is not possible and execution is not imminent, it may be best to portray passive cooperation. In addition, individuals should display a non-threatening but non-submissive posture; this may diminish physical abuse or even execution by undisciplined captors. During the initial stages of captivity, tension levels will be high and captors often feel vulnerable. Isolated persons can reduce this tension level by controlling their emotions, following instructions as far as practical, and when warranted, avoiding physical resistance. Sudden movement or action could precipitate a deadly response. To help de-escalate the situation, isolated persons should remain calm and courteous and maintain a posture of personal dignity and innocence. The mission for a hostage is to stay alive, resist exploitation, and prepare to escape.

**Captivity Survival.** Capture shock is real; injury, fear, dehydration, and purposeful captor exploitation efforts may compound its effects on captives. The captive needs to recover from its effects quickly, stay fit, and maintain or improve their physical condition to the best extent possible. It is best to exercise, including isometrics, to keep muscles ready to respond when needed. The captive should eat and drink all the sustenance captors provide and ask for more. Maintain presence of mind and constant awareness. This will allow the individual to mentally recover and begin taking actions that will be beneficial.

**Countering Denial and Deception.** The USG and its allies will employ a wide range of capabilities in an attempt to locate and identify missing, captured, and detained personnel. However, captors may employ tactics and techniques to deceive or confuse U.S. and allied efforts. This includes holding captives in unknown locations, covertly moving the captives between holding locations, and not allowing anyone from outside the captivity environment access to the captive. If a captive believes the captor is employing denial and deception, they should attempt to counter the captor's tactics by making every effort to get word out that they are alive. As stated earlier, the most accurate, efficient, and expedient means of locating an isolated individual occurs when the individual participates in providing location information to friendly/recovery forces.

**Media Exploitation.** Captors may also use print or video media reporting about captives' home units or their families' and friends' reactions to exploit captives or weaken their will to resist. Captives' family members can expect rapid and intensive media attention and should be prepared in advance with some simple guidelines to avoid supporting captors' objectives. The USG or the contractor may offer captives' families prompt personal support and guidance on public affairs; families should be encouraged to accept that support. Family members and friends should avoid speculating about captives' activities or disclosing personal information. Brief statements of support for the captive, hope for their safe return, and faith in the USG to bring the captive home are less likely to support captors' objectives of weakening a captive's will or hope.

**Proof of Life.** If the captive is not able to communicate their condition or capture to friendly forces, it may be beneficial for the captive to develop a contingency plan if the

captor decides to photograph or videotape them. With increased accessibility to technology and ease of means for posting to social media sites, it is common for captors to post pictures and/or video of the captive to the internet. Often the video or photograph supports the captors' intent to provide proof of capture, or as part of an attempt to exploit a ransom, a proof of life. The video may be exploitative in intent; however, any released pictures/video can assist in establishing a proof of life or conditions of captivity. A proof of life must contain enough specific evidence within a video, audio recording, or image to allow analysts to determine a specific date of production, verification of proof of life, and establishes a person remains alive on a specific date. The captive should try to provide a verifiable date (e.g., holding a newspaper with the front page clearly visible, clearly present a recent letter from a family member, or some other method for verifying the date) when posing for a photograph or making a video. If allowed to speak, captives should state the date and refer to a recent, verifiable event (e.g., natural disaster, diplomatic visit, sport result). In addition, the captive should indicate their physical condition and provide some information on the conditions of captivity. The captive should face the camera squarely and present a clear recording of their face while taking steps to reduce, minimize, and mitigate any possible propaganda value.

**Human Shields.** Captors may attempt to use their prisoners as human shields to facilitate movement or prevent military actions. If exploited by force to become human shields, captives should resist and continually remind the captors of their obligations under international law. They should use an appropriate, polite manner to ask captors for protection. If compliance is forced, captives should develop a strategy to make their presence known by remaining in the open and/or constructing discreet GTAS as previously described. Captives should locate and stay close to a protected area in the event the area comes under attack or if a recovery operation commences and remain alert for escape opportunities.

**General Authorized Communication Guidance.** The USG authorizes captive personnel to identify themselves; seek their government's assistance; request return to friendly control; discuss issues related to health, welfare, and treatment; and discuss the innocent circumstances leading to capture. Personnel should request contact with U.S. or supporting allied authorities while politely and persistently requesting improvements in all captives' care, treatment, and protection. Take advantage of any allowed communication medium, but be aware of providing too much exploitable information.

**Specific Guidance for Communicating with Hostage-Takers.** Personnel should communicate with captors by emphasizing the innocent, humanitarian nature of their activities, how they are trying to help and protect the people, and that their activities warrant God's mercy. One example is, *"I am separated from my unit. I am trying to help your people. I request assistance in contacting people that will help in getting me home."* Personnel should resist disclosing further information to the utmost of their ability. If personnel unwillingly or accidentally disclose sensitive information, attempt to recover and resist with a fresh line of defense (bounce back). Personnel may benefit by building rapport with their captor by garnering a simple gesture of human kindness, improved living conditions, better treatment, additional food and water or, in more

extreme cases, protection from harm or assistance. In talking with the captors, personnel should use their name and talk about non-sensitive topics and commonalities to humanize themselves. Avoid argumentative discussions on emotionally charged topics like religion and politics. Many societies respect displays of courage, tolerance of pain, religious piety, and devotion to family.

**Building Rapport.** Building rapport is the *planned, purposeful, and deliberate* establishment of a relationship with a captor so the captor sees the captive as a person rather than a symbol. Through building rapport, the captive can also convey to the captor(s) their personal dignity. This strategy may be effective in reducing tensions with captors, especially at critical times (when they issue demands or engage in deadlocked discussions). Some captors will be more amicable or receptive than others. Captives should weigh the risks and potential benefits of approaching individual captors and modify their approaches accordingly. Captives may discuss non-substantive topics to convey their human qualities and build rapport by:

- Introducing commonalities such as family, clothes, sports, hygiene, food, etc.
- Active listening -- allowing captors to discuss their cause or boast, but not praising, pandering, participating, or debating with them.
- Addressing captors by name.
- Being careful about whining or begging as it may increase abuse.
- Introducing benign topics at critical times (impasses, demands) to reduce tensions.
- Avoiding emotionally charged topics of religion, economics, and politics.
- Avoiding being singled out by being argumentative or combative.
- Avoiding escalating tensions with language such as “gun, kill, punish,” etc.

**Captor Exploitation.** The value of a captive is directly proportional to the goal(s) of a captor group. Any level of exploitation will vary according to the group’s strategic and tactical objectives. Hostage taking is a significant propaganda tool. It can change the dynamics of political conflict by giving the hostage-takers attention, instant recognition, and credibility. Most hostage-takers hold hostages in an attempt to extract money and gain concessions from governments. Objectives of hostage-takers may include: 1) promoting terror and creating fear, 2) taking advantage of the fact they have a U.S. or allied hostage by focusing their exploitation on ransom for money to help finance the group’s operations, 3) legitimizing their cause by forcing the individual’s government to recognize the captor group or 4) gain concessions from an allied nation, such as stop participation in operations against the captor group.

**Interrogation.** Governmental captors will likely interrogate detainees individually. The primary purpose will likely be to obtain operational, military, or intelligence information from the captive. Tactical interrogations will often focus on identifying the location and intentions of allied forces and/or other threats to the captors’ immediate security. Hostages should also expect questioning about their ransom value and who would be able



to pay for their release. Interrogators may employ almost all the basic interrogation methods. Inexperienced interrogators will usually apply a direct approach, possibly resorting to threats and physical abuse and death threats for results. Captors may also employ non-violent methods to extract information.

**Propaganda.** Captors may exploit captives to obtain recorded apologies, admissions, confessions, and other discrediting statements. Hostage-takers use video recordings of hostages for recruiting and garnering domestic and international support for their causes. In other countries, hostage takers have allowed journalists to interview and videotape hostages, while attempting to show good treatment, promote their cause, and put political pressure on governments for concessions. Elsewhere, captors have exploited Western hostages by video recording them voicing the terrorists' demands and making appeals to their governments or employers to resist/stop supporting America's policies/activities in the country/region.

**Indoctrination.** Captors that are more sophisticated may attempt to engage captives in political, cultural, economic, or religious discussions to indoctrinate the captive and educate them regarding the captors' ideology and grievances, or to provide justification for the individual's abduction. The captor may try to introduce the captive to a high-ranking leader when attempting this subtle tactic. In numerous other detention situations worldwide, captors tried to engage captives in political discussions and the isolated person received lectures describing historical justification.

**Resisting Exploitation.** Personnel must keep faith with their country, fellow isolated personnel, and themselves by resisting the captor. Returnees from numerous captivity situations noted personal resistance victories and bouncing back were important factors in coping with captivity and maintaining successful resistance. They felt their ability and confidence to avoid exploitation strengthened after successfully withholding information and resisting their captors. During interrogation, the captive should avoid providing full, complete, and accurate information.

**Will to Resist.** In all captivity situations, personnel have a duty to resist exploitation. Even without prior training, captives analyzed their own particular circumstances and successfully developed resistance postures and employed a variety of resistance techniques. They remarked that resistance is a matter of will; a captive who has a will to resist and makes the necessary effort can return home with honor. Personnel should view resistance to exploitation as a battle of wills, not a battle of wits. Engaging in a battle of wits is counter-productive to effective resistance. Demonstrating a strong will to resist, combined with appropriate resistance posture, can convince a captor that the individual will resist each attempt at exploitation and are an unattractive target for further attempts.

**Resisting Propaganda.** The captive should avoid situations designed for propaganda purposes whenever possible. Personnel should realize blatant resistance is likely to bring severe reprisals; however, it may be necessary on occasion. The captive is not in a good position to determine the target audience of the propaganda, which may include other captives, the captor group's own members, terrorist recruiters, non-aligned persons, or

international public opinion. While successfully minimizing the propaganda for one audience, the tactic used may have little or no effect on a separate target audience.

**Resisting Indoctrination.** It is best to avoid political, cultural, economic, and religious debate. Such debate is usually futile and not recommended for hostages and detainees. Former captives have related that adopting a willingness to listen to the captor's point of view without offending or engaging in thoughtful debate reduces tensions. Captives should attempt to discourage further discussions. Captives should focus communications on non-sensitive topics such as health and welfare issues.

**Release.** There are a number of reasons that may lead to the release of a captive by a terrorist group or from governmental detention. A hostage-taking group may not be able to care for and maintain the security and logistical support to hold their captive leading to release. Another reason for release may be that the captor group may have achieved their strategic or tactical goal, such as receiving ransom, gaining political power, prestige, concessions, or other demands. Governmental detention will likely be resolved through diplomatic contacts; this process may take time. Detainees must avoid acts considered crimes under the countries' laws that will complicate a diplomatic release. The detainee may not be aware of the conditions of release and must leave the terms of release in diplomatic channels. Captives should accept release, unless doing so requires them to compromise their honor, or causes damage to their nation or its allies. If applicable and possible, individuals should seek the senior ranking captive's guidance or approval before accepting release. Captive senior leaders in charge of captured U.S. and allied personnel should authorize the release of their personnel under almost all honorable conditions. Personnel must carefully assess their captor, their motives, and the viability of their threats if they place conditions on the release.

**Rescue from Captivity.** All captives should plan for possible rescue. During any rescue attempt, captives should move to the safest area available and avoid doors, windows, and open areas. They should drop to the floor, lie against an interior wall, and keep hands visible. They should not attempt to "help" rescue forces. Some captors may disguise captives in enemy clothing. In this case, it is imperative the captives identify themselves in a non-threatening manner to the recovery force. Captives should act extremely docile, identify the location of other known captives, and follow the rescuer's instructions. Captors may try to prevent the recovery and attempt to kill the captive in response to a rescue effort. Captives must be prepared to protect and defend themselves from a captor adopting this tactic. Additionally in a long-term captivity, the captive's appearance may change as a result of weight loss, hair growth (facial, head hair) or hair color. Rescue forces may handle unidentified captives roughly until authentication is accomplished or until they have the rescued individual secured in a safe area.

**Escape.** While in captivity, captives must develop an escape mindset to assist in preparing, planning, and executing an escape. This includes thinking about, looking for, and considering opportunities for escape. Captives should develop escape plans and contingencies, communicate with other captives, and collect material that will aid in escape and evasion. Planning for an escape should begin as soon as possible after

coming under the control of terrorists to improve their chances of escape if attempted. This planning should include the passive collection of information on the captors, the strengths and weaknesses of the facility and its personnel, the surrounding area and conditions that could have an impact on an escape attempt, and items and materials within the detention area that may support an escape effort. This alertness and continual planning for escape places a captive in the best position to exploit, facilitate, or provide assistance during an escape opportunity. The decision to escape should be based on the careful consideration of the unique circumstances of the situation, to include an assessment of the potential for success, risk of violence during the escape attempt and potential retaliation if recaptured, and consequences for captives remaining behind.

## **Guidance for Detention by Hostile Governments (Detainee)**

DoD personnel must be aware that the basic protections available to prisoners of war under the third Geneva Convention (Geneva Convention Relative to the Treatment of Prisoners of War) may not be provided, as these protections apply only during declared war or international armed conflict. Otherwise, combatants will receive only the minimum protections of Common Article 3 of the Geneva Convention. As a result, detained DoD personnel may be subject to the domestic criminal laws of the detaining nation. For example, if a U.S. person kills a civilian to avoid detection by a hostile force, the individual may face prosecution under the laws of the detaining nation. In addition to the Geneva Conventions, there may also be a status of forces agreement or some other binding agreement that provides certain parameters for the duties of the detaining government. Detainees should attempt to maintain military bearing, if possible, and should avoid aggressive or combative behavior that would violate the criminal or civil laws of the subject country. However, detainees should not forget that they have an inherent right of self-defense. DoD personnel must be prepared to assess the dangers associated with being taken into captivity by local authorities. Their assessment of the dangers should dictate what efforts should be taken and what measure of force may be required to avoid capture, resist apprehension, and resist cooperation once captured.

- Governments are obligated to notify the detainee's consular officials. As U.S. citizens, detainees should immediately and continually ask to see U.S. Embassy personnel or a representative of an allied or neutral government.
- Escape attempts from governmental detention are not recommended, except under unique or life-threatening circumstances. Although escape is considered a last resort, it may become necessary if conditions deteriorate to the point that the risks associated with escape are less than the risks of remaining captive. These risks would include the death of detainees due to treatment by the detainers or the credible threat of death or torture of the detainees by the detainers. Because escape from government detention is a crime in most countries, a failed escape attempt may provide the detainer with further justification to prolong detention by adding additional criminal or civil charges. This would be particularly true if detaining government personnel or civilians were wounded or killed during an escape by or because of the detainee. A detainee in this case may be subjected to severe punishment at the hands of the detainer's legal system that may result in bodily harm or even death to the detainee.

## **Guidance for Captivity by Terrorists (Hostage)**

Capture by terrorists is generally the least predictable and structured form of captivity. The captor may qualify as an international criminal. Tension levels will be extremely high during the initial seizing of hostages. Terrorists will likely feel most vulnerable at this point. Hostages should reduce this tension level by controlling their emotions, following instructions as far as practicable, and avoiding physical resistance. Sudden movement or action could precipitate a deadly response.

- One recommendation is for military personnel to obtain a U.S. tourist passport to assist in blending in with other travelers and to delay the initial identification process in a hostage situation. Surrender the tourist passport if the terrorists demand identification during the initial stage, or delay identification as a U.S. military or official traveler by claiming inability to locate the documents. If directly confronted about the DoD status, lying is not recommended. The initial delay serves only to maximize survival during the initial stage.
- Hostages should leave evidence of their presence whenever and wherever possible. Leaving fingerprints can assist in locating hostages. DNA, in the form of hair strand with root or drops of blood, should also be inconspicuously deposited when feasible.
- Escape from terrorists is risky but may become necessary if conditions deteriorate to the point that the risks associated with escape are less than the risks of remaining captive. These risks would include torture, the death of hostages due to treatment or the credible threat of death.

## **Taken Hostage -- You Can Survive!**

If you are taken hostage, remember your personal conduct can influence treatment in captivity. The Department of State has responsibility for the protection of all U.S. government (USG) personnel and their dependents, other than those personnel under the command of a U.S. area military commander. If kidnapped and taken hostage, the hostage has three very important rules to follow:

- Analyze the problem so as not to aggravate the situation.
- Make decisions to keep the situation from worsening.
- Maintain discipline to remain on the best terms with the captors.

### **PREPARING THE FAMILY**

- Have your family affairs in order, including a current will, appropriate powers of attorney, and measures taken to ensure family financial security.
- Issues such as continuing the children's education, family relocation, and disposition of property should be discussed with family members.
- Your family should know that talking about your official affiliation to non-DoD people may place you, or them, in great danger. Family members should consult with the local public affairs office prior to talking with media or answering any questions.

### **STAY IN CONTROL**

- Regain your composure as soon as possible and recognize your fear. Your captors are probably as apprehensive as you are, so your actions are important.
- Take mental notes of directions, times of transit, noises, and other factors to identify your location.
- Note the number, physical description, accents, habits, and rank structure of your captors.
- Anticipate isolation and efforts to disorient and confuse you.
- To the extent possible, try to mentally prepare yourself for the situation ahead. Stay mentally active.
- Attempt to secretly leave fingerprints or DNA material (e.g., hair strand with root, drop of blood) in vehicles or places where you are held.
- Your captors must be convinced the USG will work to obtain your safe release.
- Do not be depressed if negotiation efforts appear to be taking a long time. Remember that your chances of survival actually increase with time.

### **DEALING WITH YOUR CAPTORS**

- Do not aggravate them.
- Do not get into political or ideological discussions.

- Comply with instructions, but always maintain your dignity. Obedience to orders or commands need not be swift, cheerful, or overtly enthusiastic, but it should be sufficient to maintain a balanced relationship between the hostages and their captors.
- Talk in a normal voice. Avoid whispering when talking to other hostages or raising your voice when talking to a terrorist.
- Attempt to develop a positive relationship with them. Identify those captors with whom you can communicate and attempt to establish a relationship with one or more of them.
- Be proud of your heritage, government, and military association, but use discretion.

### **KEEP OCCUPIED**

- Exercise daily.
- Read anything and everything.
- Eat what is offered to you. You must maintain your strength.
- Establish a slow, methodical routine for every task.

### **BEING INTERROGATED**

- If you need to avoid answering questions to protect sensitive information, take a simple, tenable position you will be able to remember and maintain.
- Be polite and keep your temper.
- Give short answers. Talk freely about nonessential matters, but be guarded when conversations turn to matters of substance.
- Do not be lulled by a friendly approach. Remember that one terrorist may play “good guy” and one “bad guy.” This is the most common interrogation technique.
- Avoid emotionally charged topics of religion, economics, and politics.
- If forced to present terrorist demands to authorities, in writing or on tape, state clearly that the demands are from your captors.
- Avoid making a plea on your behalf.

### **DURING RESCUE**

- Drop to the floor and be still. Avoid sudden moves. Wait for instruction.
- Once released, avoid derogatory comments about your captors; such remarks will only make things harder for those still held captive.

## Personal Data

Law enforcement agencies need timely and accurate information in the event of an emergency. *When filled in, separate these pages from the guide and maintain in a secure place, ready to give to the appropriate security officials. Also, ensure this is safeguarded or destroyed as updated to protect against identity theft or compromise.*

Military personnel, DOD civilians and contractors are required to fill out DD Form 1833, Isolated Personnel Report, before deploying. While much of the same material requested below appears on the DD Form 1833, it is a classified document when completed and will not be available to local law enforcement or other non-DOD agencies.

### MILITARY MEMBER or DoD EMPLOYEE

### SPOUSE

Full Name: _____	_____
Passport Number: _____	_____
SSN: _____	_____
Rank: _____	_____
Position: _____	_____
Home Address: _____	_____
_____	_____
Phone: _____	_____
Place of Birth: _____	_____
Date of Birth: _____	_____
Citizenship: _____	_____
Race: _____	_____
Height: _____	_____
Weight: _____	_____
Build: _____	_____
Hair Color: _____	_____
Color Eyes: _____	_____
Scars/Marks/Tattoos: _____	_____
Languages Spoken: _____	_____
Medical Requirements _____	_____
Medication Required/Intervals: _____	_____
Provide Three Signature Samples:	
1. _____	_____
2. _____	_____
3. _____	_____

Attach two photographs, one full-length front view, and one full-length side view. Attach one complete fingerprint card. It is also prudent to have an audio recording of the person's voice and a DNA sample.



**CHILD 1**

**CHILD 2**

Full Name: \_\_\_\_\_

Passport Number: \_\_\_\_\_

SSN: \_\_\_\_\_

Home Address: \_\_\_\_\_

\_\_\_\_\_

Phone: \_\_\_\_\_

Place of Birth: \_\_\_\_\_

Date of Birth: \_\_\_\_\_

Citizenship: \_\_\_\_\_

Race: \_\_\_\_\_

Height: \_\_\_\_\_

Weight: \_\_\_\_\_

Build: \_\_\_\_\_

Hair Color: \_\_\_\_\_

Color Eyes: \_\_\_\_\_

Scars/Marks/Tattoos: \_\_\_\_\_

Languages Spoken: \_\_\_\_\_

\_\_\_\_\_

Medical Requirements or

Problems: \_\_\_\_\_

Medication Required and

Time Intervals: \_\_\_\_\_

Provide Three Signature Samples:

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

*Warning: Separate these pages from the guide and maintain in a secure place, ready to give to the appropriate security officials. Also, ensure this information is safeguarded or destroyed as updated to protect against identity theft or compromise.*

**CHILD 3**

**CHILD 4**

Full Name: \_\_\_\_\_

Passport Number: \_\_\_\_\_

SSN: \_\_\_\_\_

Home Address: \_\_\_\_\_

\_\_\_\_\_

Phone: \_\_\_\_\_

Place of Birth: \_\_\_\_\_

Date of Birth: \_\_\_\_\_

Citizenship: \_\_\_\_\_

Race: \_\_\_\_\_

Height: \_\_\_\_\_

Weight: \_\_\_\_\_

Build: \_\_\_\_\_

Hair Color: \_\_\_\_\_

Color Eyes: \_\_\_\_\_

Scars/Marks/Tattoos: \_\_\_\_\_

Languages Spoken: \_\_\_\_\_

\_\_\_\_\_

Medical Requirements or

Problems: \_\_\_\_\_

Medication Required and

Time Intervals: \_\_\_\_\_

Provide Three Signature Samples:

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

*Warning: Separate these pages from the guide and maintain in a secure place, ready to give to the appropriate security officials. Also, ensure this information is safeguarded or destroyed as updated to protect against identity theft or compromise.*

**AUTOMOBILES OR RECREATIONAL VEHICLES**

Make and Year: \_\_\_\_\_

Color: \_\_\_\_\_

Model: \_\_\_\_\_

Doors: \_\_\_\_\_

Style: \_\_\_\_\_

License/State: \_\_\_\_\_

Vehicle ID: \_\_\_\_\_

Distinctive Markings: \_\_\_\_\_

Make and Year: \_\_\_\_\_

Color: \_\_\_\_\_

Model: \_\_\_\_\_

Doors: \_\_\_\_\_

Style: \_\_\_\_\_

License/State: \_\_\_\_\_

Vehicle ID: \_\_\_\_\_

Distinctive Markings: \_\_\_\_\_

Make and Year: \_\_\_\_\_

Color: \_\_\_\_\_

Model: \_\_\_\_\_

Doors: \_\_\_\_\_

Style: \_\_\_\_\_

License/State: \_\_\_\_\_

Vehicle ID: \_\_\_\_\_

Distinctive Markings: \_\_\_\_\_

*Warning: Separate these pages from the guide and maintain in a secure place, ready to give to the appropriate security officials. Also, ensure this information is safeguarded or destroyed as updated to protect against identity theft or compromise.*

## **Antiterrorism Points of Contact**

**For additional information, contact your antiterrorism office:**

**Assistant Secretary of Defense:**

(Homeland Defense & American Security Affairs)  
2600 Defense Pentagon Room 5D414  
Washington, D.C. 20301-2600  
(703) 697-5664/DSN: 227-5664

**The Joint Staff:**

Attn: J-3/DDAT/HD; AT/FP Div  
NMCC, The Pentagon  
Washington, D.C. 20318-3000  
(703) 697-9444/DSN: 227-9444

**Army:**

Headquarters Department of the Army  
DAPM-OPS-AT  
2800 Army Pentagon  
Washington, D.C. 20310  
(703) 695-4912/DSN: 225-4912

**Marine Corps:**

Headquarters, USMC  
Mission Assurance Branch  
Room 4A324-26, The Pentagon  
Washington, D.C. 20380-1775  
(703) 692-4235/DSN: 222-4235

**Navy:**

Chief of Naval Operations (N3AT)  
2000 Navy, The Pentagon  
Washington, D.C. 20350-2000  
(703) 614-9299/DSN: 288-0949

**Air Force:**

Headquarters U.S. Air Force  
Force Protection & Operations Division (A7SO)  
1030 Air Force Pentagon, 4A1076  
Washington, D.C. 20330-1340  
(571) 256-0474/DSN: 260-0474

(INTENTIONALLY BLANK)

(BACK PAGE)  
(Last Page of Document)