

**Military Police**  
**FORSCOM High Risk Personnel Security Program**

---

**History.** This is the first printing of FORSCOM Regulation 190-58.

**Summary.** This regulation establishes the FORSCOM High Risk Personnel Security Program and provides MACOM guidance to DOD/HQDA policy. The FORSCOM High Risk Personnel (HRP) Security Program is a component of the FORSCOM Force Protection Program.

**Applicability.** This regulation applies to all FORSCOM assigned and attached active and reserve Army units.

**Supplementation.** This regulation may be supplemented without prior approval from HQ, FORSCOM.

**Forms.** Only forms ending with the suffix "-R" may be reproduced locally on 8 1/2 x 11 inch paper through the servicing forms management office. Other forms will not be reproduced; they will be ordered by unit or organization publications officer from FORSCOM Publications and Forms Branch, or as stated in the authorizing directive. Only ".E" forms will be generated electronically (AR 25-30, para 3-3 and 3-16).

**Interim Changes.** Interim changes to this regulation are not official unless authenticated by DCG/CofS, FORSCOM. Interim changes will be destroyed on their expiration dates unless sooner superseded or rescinded.

**Suggested Improvements.** The proponent of this regulation is Provost Marshal, HQ, FORSCOM (AFPM-FP), (404) 464-5909. Users may send comments and suggested improvements to this publication on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, FORSCOM, ATTN: AFPM-FP or via electronic mail to [fp-officer@forscom.army.mil](mailto:fp-officer@forscom.army.mil)

**Distribution.** Distribute according to DA Form 12-88-E, block 0235, Command level A.

**Restrictions.** This regulation is approved for public release with unlimited distribution. Local reproduction authorized.

OFFICIAL: **//Signed//**  
LAWSON W. MAGRUDER III  
Lieutenant General, USA  
Deputy Commanding General/  
Chief of Staff

**SIGNED**  
JAMES G. VAN PATTEN  
Colonel, GS  
Assistant Deputy Chief of Staff for  
Command, Control, Communications  
and Computers

**DISTRIBUTION:** Distribution is intended for command level A.

**Copy Furnished:** HQ FORSCOM (AFCI-A) (record copy).

---

**TABLE OF CONTENTS**

|                                            |          |                                             |          |
|--------------------------------------------|----------|---------------------------------------------|----------|
|                                            |          | <b>Abbreviations and Terms</b>              | <b>3</b> |
| <b>Chapter 1</b>                           | <b>3</b> |                                             |          |
| <i>General</i>                             | <b>3</b> |                                             |          |
| <b>1-1. Purpose</b>                        | <b>3</b> | <b>1-4. Personal Security Vulnerability</b> |          |
| <b>1-2. References</b>                     | <b>3</b> | <b>Assessment Checklist</b>                 | <b>3</b> |
| <b>1-3. Individual Protective Measures</b> |          | <b>1-5. Overview</b>                        | <b>3</b> |

**FORSCOM Regulation 190-58**

|                                                           |          |
|-----------------------------------------------------------|----------|
| <b>1-6. Designation of High Risk Personnel</b>            | <b>3</b> |
| <b>1-7. Requirements</b>                                  | <b>3</b> |
| <b>Chapter 2</b>                                          | <b>5</b> |
| <i>Personal Security Vulnerability Assessments (PSVA)</i> |          |
| <b>2-1. General</b>                                       | <b>5</b> |
| <b>2-2. Requirements</b>                                  | <b>5</b> |
| <b>Chapter 3</b>                                          | <b>6</b> |
| <i>Protective Service Details (PSD)</i>                   |          |
| <b>6</b>                                                  |          |
| <b>3-1. General</b>                                       | <b>6</b> |
| <b>3-2. Planning and Equipping</b>                        | <b>6</b> |
| <b>3-3. Full-time Protective Service</b>                  | <b>6</b> |
| <b>Chapter 4</b>                                          | <b>7</b> |
| <i>Hardened (Armored) vehicles</i>                        |          |
| <b>4-1. General</b>                                       | <b>7</b> |
| <b>4-2. Request for HAV Support</b>                       | <b>7</b> |
| <b>4-3. Request for LAV Support</b>                       | <b>7</b> |
| <b>4-4. Disposal of HAV/LAV</b>                           | <b>7</b> |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <b>Chapter 5</b>                                                   |           |
| <i>Domicile to Duty Transportation</i>                             |           |
| <b>5-1. General</b>                                                | <b>8</b>  |
| <b>5-2. Request for D-T-D Authorization</b>                        | <b>8</b>  |
| <b>Appendix A</b>                                                  | <b>9</b>  |
| <i>References</i>                                                  |           |
| <b>Appendix B</b>                                                  | <b>11</b> |
| <i>Individual Protective Measures</i>                              |           |
| <b>Appendix C</b>                                                  | <b>18</b> |
| <i>Personal Security Vulnerability Assessment (PSVA) Checklist</i> |           |

## **CHAPTER 1**

### ***General***

#### **1-1. Purpose**

This regulation:

- a. Implements requirement in Army Regulation 190-58 for major Army command (MACOM) commanders to establish a High Risk Personnel (HRP) Security Program.
- b. Prescribes policy/procedures and assigns responsibilities for developing and maintaining a practical, economic, and effective FORSCOM high risk personnel security program to safeguard high risk personnel and their family members.
- c. Prescribes standards for security of HRPs.

#### **1-2. References**

Required and related publications and referenced forms are listed in **Appendix A**.

#### **1-3. Individual Protective Measures Abbreviations and Terms**

Individual protective measures are listed in **Appendix B**.

#### **1-4. Personal Security Vulnerability Assessment (PSVA) Checklist**

A PSVA checklist is located at **Appendix C**.

#### **1-5. Overview**

Personnel who by virtue of their rank, assignment, symbolic value, vulnerabilities, location or specific threat, are at greater risk than the general population, will be designated as "high risk personnel".

#### **1-6. Designation of High Risk Personnel**

- a. There are two designated levels of high-risk personnel (HRP). Level I HRP are those individuals who have such a significantly high potential as terrorist or criminal targets as to warrant assignment of full-time protective services details. Level II HRP personnel do not warrant assignment of full-time protective services but require additional office, residential, and/or travel security measures. Justification for designation as HRP will be based on assessment of both the threat and individual vulnerabilities. Justification as a HRP may also be based on an individual's assignment to a designated high-risk billet (HRB).
- b. Only the FORSCOM commander may designate HRP as Level I. The authority to designate HRP as Level II may be delegated to installation commanders by the FORSCOM commander. Installations commanders will submit an annual report NLT 1 November to HQ, FORSCOM (AFPM), listing all Level I and II HRP within their geographical areas of responsibility effective 1 October of each year. Changes to Level I HRP lists will be reported within 14 days to HQ, FORSCOM (AFPM). All reports will be appropriately classified and include the position of HRP (if designation is based on HRB), incumbent's name (or name of individual whose designation is not based on a HRB), and location (installation, military community, or city).

#### **1-7. Requirements**

- a. Commanders will identify personnel who qualify as HRP and will formally designate and protect those individuals IAW this regulation. The levels of protection and types of security measures afforded to HRP will be determined by both threat and vulnerability assessments.
- b. Designated HRP and their family members will be made aware of risks and trained in appropriate personal protective measures they can apply.
- c. Commanders will employ appropriate security measures to provide enhanced protection to HRP. Reviews of supplemental security needs are undertaken immediately upon a change in THREATCON, or receipt of specific targeting information. See Appendix 1 for examples of security measures.
- d. At installation level, commanders will establish formal HRP security programs that include written procedures:

**FORSCOM Regulation 190-58**

- (1) For the review of personnel as potential HRP
- (2) Training requirements for HRP, their family members, and supporting staffs where applicable
- (3) Employment of appropriate physical and procedural security measures
- (4) Designation of appropriate personnel as HRP

## CHAPTER 2

### *Personal Security Vulnerability Assessments (PSVA)*

#### 2-1. General

PSVA will be conducted to assess the security posture of HRP. The assessment will identify potential vulnerabilities and recommend corrective actions. PSVA are the basis upon which HRP security measures will be developed and employed. See Appendix C for PSVA checklists.

#### 2-2. Requirements

- a. PSVA is mandatory for all Level I HRP.
- b. All Level II HRP will be offered a PSVA.
- c. Upon designation as a HRP, an initial PSVA will be conducted. A PSVA will be performed by the supporting USACIDC office for HRP as directed by HQDA and/or coordinated with supported commands. A PSVA is intended to identify security weaknesses in the individual's living and working environments, travel between those locations, and the HRP's personal activities, and identify measures to correct those weaknesses. The PSVA will be reviewed at least annually thereafter and also when there is a substantial change in the threat. Surveys will include, as a minimum, a review of procedures/measures employed at the HRP's quarters, work place and travel between the two locations.

## CHAPTER 3

### *Protective Service Details (PSD)*

#### 3-1. General

- a. The objective of protective service details is to provide dedicated security to personnel who have been identified as HRP. This security can be provided on either a full or part-time basis depending on the situation. Protective service details deter, detect and defend against threats to the principal. The mission of protective services is to protect the principle from assassination, kidnapping, injury, and embarrassment. Protective services personnel must be able to react instantly by covering and removing the principal in case of attack or risk situations. Personnel performing protective services duties for Level I HRP are selected using criteria in AR 190-58. Additionally, Protective Service Details (PSD) will be trained, organized, and equipped IAW AR 190-58.

- b. Protective services operations will be conducted in accordance with U.S. laws and regulations and international agreement. Unless authorized by statute, soldiers performing personal protective services off military installations will not identify themselves as law enforcement agents or wear accouterments that project military law enforcement authority. Military personnel may not enforce civilian law, however, they will act to defend the HRP or themselves wherever they may be.

- c. Conduct of protective services, organization of the protective service force, the number of personnel employed, and the duration of the mission will be determined based on the status of the principal, threat, vulnerabilities, location and other conditions that may present a danger to the principle being protected.

#### 3-2. Planning & Equipping

- a. Protective services will be based on a defense in depth employing concentric cordons of security. The inner cordon normally consists of dedicated full-time protective services personnel assigned to protect the principal. Outer cordons will be located based on threat and vulnerabilities. This may include uniformed and non-uniformed security personnel and/or physical barriers.

- b. Responsibilities will be clearly defined throughout any protective service mission. Escort officers, aides, protocol officers, and security personnel will be clearly identified and assigned responsibilities.

- c. Duties of protective service details may include:

- (1) Advance security coordination and surveys preceding the principal.
- (2) Accompanying the principal when traveling.

## **FORSCOM Regulation 190-58**

- (3) Guarding residence or office.
- (4) Protective counter-surveillance of the principal.
- d. Standard Army weapons and equipment will be used to the extent practical. Execution of protective service missions may however require the use of special materials and equipment. If items are not provided by TOE and TDA authorizations, or through routine supply channels, commanders may utilize local purchase or lease.
- e. Full-time protective service teams are authorized use of unmarked vehicles of commercial design and colors in performance of their official duties. TDA authorities will provide a minimum of two vehicles for team use for each principal being protected. Vehicles should be similar to those available on the local economy but will be IAW AR 58-1.
- f. Protective service details will normally be equipped with securable radios, which have hands-free operational capability. Radio security will be IAW Federal Standard 1027 and AR 530-2.
- g. Contingency limitation .0015 funds are available for extraordinary and emergency expenditures in excess of Joint Federal Travel Regulation authorizations to support full-time protective service requirements. These funds are administered by USACIDC in compliance with AR 195-4. The local Criminal Investigation Command element will be coordinated with prior to obligation or expenditure of .0015 funds.

### **3-3. Protective Service Detail Qualifications**

- a. Personnel performing protective service duties will:
  - (1) Be qualified in MOS 95B, Military Police or 95D, Criminal Investigation Division special agent.
  - (2) Be in pay grade E-5 or above.
  - (3) Have at least a SECRET clearance.
  - (4) Be free of any record reflecting civilian or military offenses other than minor violations listed in AR 602-210 (Qualifications for Military Policeman) and other conduct or behavior not in the best interest of Army law enforcement.
  - (5) Be cleared by a favorable U.S. Army Crime Records name check.
  - (6) Be in excellent physical condition, to include passing their most recent Army Physical Fitness Test and conforming to the height and weight standards in AR 600-9.
  - (7) Complete the U.S. Army Military Police School Counter-Drug Anti-Terrorism Personal Protection Course or other properly certified course offered by local, state, or Federal law enforcement agencies.
- b. Commanders nominating an individual for full-time protective service duties will dispatch a message to DIR USACRC //CICR-RT// FT BELVOIR VA requesting a name check. Information copies of the request will be provided the FORSCOM Provost Marshal and the Commander, PERSCOM, ATTN: TAPC-PDS, Alexandria, VA. The request will include the following information:
  - (1) Candidate's full name (include former names and maiden names).
  - (2) Candidates social security number.
  - (3) Candidate's place of birth.
  - (4) Candidate's date of birth.
  - (5) Candidate's primary MOS.
  - (6) Candidate's pay grade.
  - (7) Candidate's expiration term of service.
  - (8) Candidate's current security clearance.

## **CHAPTER 4**

### ***Hardened (Armored) Vehicles***

#### **4-1. General**

- a. Armored vehicles can be an essential element in the overall requirement to provide protection for HRP. Hardened vehicles provide protection during a critically vulnerable period and movement from site to site. Commercially produced, fully armored or Heavy Armored Vehicles (HAVs) are scarce and very costly resources that must be carefully managed. A light armored nontactical vehicle or Light Armored Vehicle (LAV) is not as costly but does not afford the level of protection provided by a HAV. The acquisition of hardened vehicles requires significant lead.
- b. Armored vehicles are used solely for the protection of officials in the performance of their official duties and/or at other times on the basis of specific threat assessments and vulnerability assessments, which have been

coordinated with HQ, USJFCOM. In order to use a DoD vehicle, including HAVs and LAVs, for domicile to duty transportation, a request must be submitted to HQ FORSCOM, PMO for forwarding to Secretary of the Army, who has authority for final approval in accordance with chapter 4 of DoD Directive 4500.36, Management, Acquisition, and Use of Motor Vehicles; AR 58-1, paragraph 4-4. The request, with data required and listed at AR 58-1 para4-4, will be submitted to HQDA, ATTN: DALO-TSP, for approval.

#### **4-2. Request for HAV Support**

Requests for armored vehicles will be submitted to the FORSCOM PM for validation and processing. If the request is for a HAV, the requirements in DoD 4500.51 must be met. Requests for HAVs require a detailed justification to include the following information:

- a. Manpower position the vehicle is intended for.
- b. Current/projected threat and vulnerability assessment.
- c. Current armored vehicle assets available.
- d. Whether request is a new requirement or to replace an existing vehicle.
- e. Why a LAV would not be appropriate.
- f. Funding availability.

#### **4-3. Request for LAV Support**

Requests for a LAV will include the following information:

- a. Manpower position the LAV is intended for.
- b. Current/projected threat and vulnerability assessment.
- c. What type of vehicle is requested.
- d. If request is for an add-on armor kit, include information on the vehicle to be modified (year, make, model, transmission type, whether vehicle has heavy duty radiator/suspension). Also specify whether the vehicle is in-country or being procured and shipped.
- e. Current armored vehicle assets available.
- f. Whether request is for a new requirement or to replace an existing one.
- g. Funding availability.

#### **4-4. Disposal of HAV/LAV**

Disposal of HAVs/LAVs will be accomplished in accordance with DoD C-4500.51. Formal notification of intent to dispose of HAVs/LAVs will be made to HQ FORSCOM, PMO. Notification that all the transparent armor and opaque armoring materials in vehicle windows and in the body of the vehicle have been removed from LAVs before disposal will be sent to HQ FORSCOM.

## **CHAPTER 5**

### ***Domicile to Duty Transportation***

#### **5-1. General**

31 U.S.C. 1344, as amended, governs the use of Government vehicles for domicile-to-duty (D-T-D) transportation. Requests for DTD transportation authorization, based on security reasons, must be approved by the Secretary of the Army and must establish that highly unusual circumstances present a clear and present danger. The perceived danger must be real and imminent and it must be demonstrated that use of such transportation will provide protection not otherwise available. Exceptions to prohibitions against use of government vehicles for DTD transportation may be reported to Congress by DoD and must be able to stand up to rigorous scrutiny. Requests for DTD transportation, based on security reasons, will normally be disapproved by HQ FORSCOM if the principal concerned is not designated high risk.

#### **5-2. Requests for D-T-D Authorization**

Requests for DTD transportation authorization will be submitted through the appropriate chain of command, to the FORSCOM DCSLOG. The DCSLOG will coordinate requests with the FORSCOM Force Protection Committee. The DCSLOG will complete any additional coordination that may be required and forward the requests to HQDA.

**Appendix A**  
**References**

**AR 10-23**

United States Army Criminal Investigation Command

**AR 58-1**

Management, Acquisition and Use of Administrative Use Motor Vehicles

**AR 190-11**

Physical Security of Arms, Ammunition, and Explosives

**AR 190-14**

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties.

**AR 190-30**

Military Police Investigations

**AR 190-58**

Personal Security

**AR 195-4**

Use of Contingency Limitation .0015 Funds for Criminal Investigative Activities.

**AR 525-13**

The Army Terrorism Counteraction Program

**AR 530-2**

Communications Security

**AR 600-9**

The Army Weight Control Program

**AR 601-210**

Regular Army and Army Reserve Enlistment Program

**AR 700-84**

Issue and Sale of Personal Clothing

**AR 710-2**

Supply Policy Below the Wholesale Level

**Federal Standard 1027**

Telecommunications: Federal Security Requirements Using the Data Encryption Standard.

**Section II**

***Required Publications***

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

**AR 5-3**

Installation Management and Organization

**AR 195-2**

Criminal Investigation Activities

**FORSCOM Regulation 190-58**

**AR 380-67**

Personnel Security Program.

**FM 19-20**

Law Enforcement Investigations

**FM 19-30**

Physical Security

**JFTR, Volume I**

The Joint Federal Travel Regulations, Volume I  
Uniformed Service Members.

**DA Form 5703**

Protective Service Agent

**DA Form 4187**

Personnel Action

## **Appendix B**

### ***Individual Protective Measures***

#### **B-1. Keep a Low Profile**

Your dress, conduct, and mannerisms should not attract attention. Make an effort to blend into the local environment. Avoid publicity and don't go out in large groups. Stay away from civil disturbances and demonstrations.

#### **B-2. Be Unpredictable**

Vary your route to and from work and the time you leave and return home. Vary the way you dress. Don't exercise alone. Don't exercise at the same time and place each day, or on deserted streets, or country roads. Let people close to you know where you are going, what you'll be doing, and when you should be back.

#### **B-3. Be Very Alert**

Watch for anything suspicious or out of place. Don't give personal information over the telephone. If you think you are being followed, go to a pre-selected secure area. Immediately report the incident to your force protection unit advisor, military intelligence officer, military police or law enforcement agencies. In overseas areas without these agencies, report the incident to the Security Officer or the Military Attache at the U.S. Embassy.

#### **B-4. General Security Checklist**

- a. Instruct your family and associates not to provide strangers with information about you or your family.
- b. Do not give unnecessary personal details to information collectors and restrict personal data when using the Internet.
- c. Be alert to strangers who are on government property for no apparent reason. Report all suspicious persons loitering near your residence or office; attempt to provide a complete description of the person and/or vehicle to police or security.
- d. Vary daily routines to avoid habitual patterns. If possible, vary travel times and routes to and from work.
- e. Refuse to meet with strangers outside your work place.
- f. Always advise associates or family members of your destination and the anticipated time of arrival when leaving the office or home.
- g. Don't open doors to strangers.
- h. Memorize key phone numbers - office, home, police, security, etc.
- i. Be cautious about giving out information regarding family travel plans or security measures and procedures.
- j. If you are overseas, learn and practice a few key phrases in the native language, such as "I need a policeman, doctor," etc.

#### **B-5. Residential and Family Security**

Although family members are seldom targeted by terrorists, they should practice basic precautions for their personal security. Familiarize your family with the local terrorist threat and regularly review the protective measures and techniques listed. Ensure everyone in the family knows what to do in an emergency. Most precautions are simple, common sense measures, which will help protect you from any criminal activity.

- a. Exterior grounds:
  - (1) Do not put your name or rank on the outside of your residence or mailbox.
  - (2) Have good light
  - (3) Control vegetation to eliminate hiding places.
- b. Entrances and exits should have:
  - (1) Solid doors with deadbolt locks.
  - (2) One-way peep-holes in exterior doors.
  - (3) Locks on skylights.
  - (4) Metal grating on glass doors and ground floor windows, with interior release mechanisms that are not reachable from outside.
- c. Interior features:
  - (1) Alarm and intercom system.

## **FORSCOM Regulation 190-58**

- (2) Fire extinguishers.
- (3) Medical and first aid equipment.
- d. Other desirables features:
  - (1) A clear view of approaches.
  - (2) More than one access road.
  - (3) Off-street parking.
  - (4) High (6-8 feet) perimeter wall or fence.
  - (5) Establish a family safe room.

### **B-6. Tips For the Family Members at Home**

- a. Restrict the possession of house keys. Change locks if keys are lost or stolen and when moving into a previously occupied residence.
- b. Lock all entrances at night, including the garage. Keep the house locked, even if you are at home.
- c. Destroy all envelopes or other items that indicate your name and rank.
- d. Know your neighbors.
- e. Do not draw attention to yourself. Avoid frequent exposure on balconies and near windows.
- f. Be aware of the threat level - listen to local news reports.
- g. Be Suspicious.
  - (1) Be alert to public works crews and, if overseas, other foreign nationals requesting access to your residence; verify identity through a peep-hole before allowing entry.
  - (2) Write down license numbers of suspicious vehicles; note descriptions of occupants.
  - (3) Be suspicious of inquiries about the whereabouts or activities of other family members.
  - (4) Report all suspicious activity to Military Police or local law enforcement.
- h. Telephone Security
  - (1) Post emergency numbers on the telephone
    - (a) Military Police:
    - (b) Local Police:
    - (c) Fire Department:
    - (d) Hospital:
  - (2) Do not answer your telephone with your name and rank.
  - (3) Report all threatening phone calls to security officials.

### **B-7. Special Precautions for Children**

- a. Never leave young children alone or unattended. Be certain they are in the care of a trustworthy person.
- b. Instruct children to keep doors and windows locked, and never to admit strangers.
- c. Teach children how to contact the police or a neighbor in an emergency.
- d. Know where your children are all the time.
- e. Advise your children to:
  - (1) Never leave home without telling you where they will be and who will accompany them.
  - (2) Travel in pairs or groups.
  - (3) Avoid isolated areas.
  - (4) Use locally approved play areas where recreational activities are supervised by responsible adults and where police protection is readily available.
  - (5) 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."
  - (6) Report immediately to the nearest person of authority, (parent, teacher, police) anyone who attempts to molest or annoy them.

### **B-8. Child Care Providers**

- a. Conduct a security background check with local police, neighbors, and friends. (Verify references.)
- b. Inform employees about security responsibilities.
- c. Instruct them which phone or other means of communication to use in an emergency.
- d. Do not discuss travel plans or sensitive topics within employees hearing.
- e. Discuss duties in friendly, firm manner.
- f. Give presents or gratuities according to local customs.

**B-9. Mail Packages**

- a. Suspicious characteristics to look for include:
  - (1) An unusual or unknown place of origin.
  - (2) No return address.
  - (3) An excessive amount of postage.
  - (4) Abnormal or unusual size.
  - (5) Oily stains on the package.
  - (6) Wires or strings protruding from or attached to an item.
  - (7) Incorrect spelling on the package label.
  - (8) Differing return address and postmark.
  - (9) Appearance of foreign style handwriting.
  - (10) Peculiar odor. (Many explosives used by terrorists smell like shoe polish or almonds.)
  - (11) Unusual weight.
  - (12) Uneven balance or shape.
- b. Never touch or move a suspicious package or letter.
- c. Do not cut tape, strings, or other wrappings on a suspect package or immerse a suspected letter or package in water. Either action could cause an explosive device to detonate
- d. Report any suspicious packages or mail to security officials immediately.

**B-10. When Away from Home**

- a. Leave the house with a "lived-in" look.
- b. Stop deliveries of mail and news subscriptions.
- c. Don't leave notes on doors.
- d. Don't hide keys outside house.
- e. Use a timer to turn lights on and off at varying times and locations.
- f. Leave radio on (best with a timer). Hide valuables.
- g. Notify the police or trusted neighbors of your absence.
- h. Ask friends/neighbors to physically check the residence.

**B-11. Security Overseas**

Criminal and terrorist acts against individuals usually occur outside the home and after the victim's habits have been established. Your most predictable habit is the route of travel from home to duty station or to commonly frequented local facilities.

**B-12. Ground Transportation**

- a. Travel in groups as much as possible. Avoid high-risk areas and demonstrations, and vary movements so as not to be predictable.
- b. Try to be inconspicuous when using public transportation and facilities. Dress, conduct, and mannerisms should not attract attention.
- c. Avoid public demonstrations; do not be curious.
- d. Stay away from controversial meeting places; patronize reputable establishments, but don't frequent the same off-base locations (in particular, known U.S. hangouts).
- e. Limit alcohol intake in any public place.

**B-13. Vehicles Overseas**

- a. Select a plain car; avoid the "Rich American" look. Consider not using a marked government car.
- b. Do not display decals with unit or branch affiliation or display gear in rear of vehicle.
- c. Auto maintenance:
  - (1) Keep vehicle in good repair.
  - (2) Always keep gas tank at least half full.
  - (3) Ensure tires have sufficient tread.
- d. Parking:
  - (1) Always lock your car.
  - (2) Don't leave it on the street overnight, if possible.
  - (3) Check for suspicious persons before exiting vehicle.
  - (4) Leave only the ignition key with parking attendant.

## **FORSCOM Regulation 190-58**

- (5) Don't allow entry to the trunk unless you're there to watch.
- (6) Never leave garage doors open or unlocked.
- (7) Use a remote garage door opener if available.
- (8) Enter and exit your car in the security of the closed garage.
- e. Traveling:
  - (1) Before leaving buildings to get into your vehicle, check the surrounding area for anything suspicious.
  - (2) If possible vary routes to work and home. Avoid late night travel.
  - (3) Travel with companions.
  - (4) Avoid isolated roads or dark alleys when possible.
  - (5) Habitually ride with seatbelts buckled, doors locked, and windows closed.
  - (6) Be alert while driving or riding. Do not allow your vehicle to be boxed in; maintain a minimum 8-foot interval between you and the vehicle in front; avoid the inner lanes.
  - (7) Know how to react if you are being followed:
    - (a) Circle the block for confirmation of surveillance.
    - (b) Do not stop or take other actions which could lead to confrontation. Do not drive home. Get description of car and its occupants.
    - (c) Go to the nearest safe haven.
    - (d) Report incident to military police.
  - (8) Recognize events that can signal the start of an attack, such as:
    - (a) Cyclist falling in front of your car. Flagman or workman stopping your car.
    - (b) Fake police or government checkpoint.
    - (c) Disabled vehicle/accident victims on the road.
    - (d) Unusual detours.
    - (e) An accident in which your car is struck.
    - (f) Cars or pedestrian traffic that box you in.
    - (g) Sudden activity or gunfire.
  - (9) Know what to do if under attack in a vehicle:
    - (a) Without subjecting yourself passengers, or pedestrians to harm, try to draw attention to your car by sounding the horn.
    - (b) Put another vehicle between you and your pursuer.
    - (c) Go to closest safe haven.
    - (d) Report incident to military police.

### **B-14. Commercial Vehicles**

- a. Vary mode of commercial transportation.
- b. Don't always use the same company.
- c. Don't let someone you don't know direct you to a specific commercial vehicle or carrier.
- d. Ensure vehicle is licensed, and has adequate safety equipment (seatbelts at a minimum).
- e. Ensure face of driver and picture on license are the same.
- f. Specify the route you want the driver to follow.
- g. Select busy areas for stops.

### **B-15. Air Travel**

- a. Get a threat briefing from your security officer prior to traveling in a high-risk area.
- b. Use military air or U.S. flag carriers.
- c. Avoid scheduling through high-risk areas; if necessary, use indirect routings to avoid high-risk airports.
- d. Don't use rank or military address on tickets, or hotel reservations.
- e. Select a window seat; they offer more protection since aisle seats are closer to the hijackers' movements up and down the aisle.
- f. Rear seats also offer more protection since they are farther from the center of hostile action, which is often near the cockpit.
- g. Seats at an emergency exit may provide an opportunity to escape.

**B-16. Personal Identification**

- a. Don't discuss your military affiliation.
- b. You must have proper identification to show airline and immigration officials.
- c. Consider use of a tourist passport, if you have one, with necessary visas, providing it's allowed by the country you are visiting.
- d. If you use a tourist passport, consider placing your official passport, military ID, travel orders, and related documents in your checked luggage, not in your wallet or briefcase.
- e. If you must carry these documents on your person, select a hiding place onboard the aircraft to "ditch" them in case of a hijacking.
- f. Luggage:
  - (1) Use plain, civilian luggage; avoid military looking bags such as B-4 bags and duffel bags.
  - (2) Remove all military patches, logos, or decals from your luggage and briefcase.
  - (3) Ensure luggage tags don't show your rank or military address.
  - (4) Don't carry official papers in your briefcase.
- g. Clothing:
  - (1) Travel in conservative civilian clothing when using commercial transportation or when traveling military airlift if you are to connect with a flight at a commercial terminal in a high-risk area.
  - (2) Don't wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.
  - (3) Don't wear U.S. identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.
  - (4) Wear a long-sleeved shirt if you have a visible U.S. affiliated tattoo.

**B-17. Precautions at the Airport**

- a. Arrive early; watch for suspicious activity.
- b. 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.
- c. 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.
- d. Don't linger near open public areas. Quickly transit waiting rooms, commercial shops, and restaurants.
- e. Proceed through security checkpoints as soon as possible.
- f. Avoid secluded areas that provide concealment for attackers.
- g. Be aware of unattended baggage anywhere in the terminal.
- h. Be extremely observant of your personal carry-on luggage. Luggage not properly guarded provides an opportunity for a terrorist to place an object or device in it.
- i. Observe the baggage claim area from a distance. Do not retrieve your bags until the crowd clears. Proceed to the customs lines at the edge of the crowd.
- j. Report suspicious activity to the airport security personnel.

**B-18. Hostage Survival**

The chances of you being taken hostage are truly remote. Even better news is that survival rates are high. But should it happen, remember, your personal conduct can influence treatment in captivity. The Department of State has responsibility for U.S. government personnel and their dependents in overseas areas. Should a hostage situation develop, the Department of State will immediately begin to take action according to preconceived plans to attempt to release the hostages.

**B-19. Tips to Ensure Survival**

- a. If kidnapped and taken hostage:
  - (1) Remain calm.
  - (2) Blend in with other passengers.
  - (3) Do not "take charge", you may be identified as a threat.
  - (4) Do not aggravate the situation.
- b. Actions if attacked:
  - (1) Dive for cover. Do not run. Running increases the probability of shrapnel hitting vital organs, or the head.
  - (2) If you must move, belly crawl or roll. Stay low to the ground, using available cover.

## **FORSCOM Regulation 190-58**

(3) Responding security personnel will not be able to distinguish you from attackers. Do not attempt to assist them in any way. Lay still until told to get up.

c. Actions if hijacked:

- (1) Remain calm, be polite and cooperate with your captors.
- (2) Be aware that all hijackers may not reveal themselves at the same time. A lone hijacker may be used to draw out security personnel for neutralization by other hijackers.
- (3) Surrender your tourist passport in response to a general demand for identification.
- (4) Don't offer any information; confirm your military status only if directly confronted with the fact.
- (5) Be prepared to explain that you always travel on your personal passport and that no deceit was intended.
- (6) Discreetly dispose of any military or U.S. affiliated documents.
- (7) Don't draw attention to yourself with sudden body movements, verbal remarks, or hostile looks.
- (8) Prepare yourself for possible verbal and physical abuse, lack of food, drink, and sanitary conditions.
- (9) If permitted, read, sleep, or write to occupy your time.
- (10) Discreetly observe your captors and memorize their physical descriptions. Include voice patterns and language distinctions, as well as clothing and unique physical characteristics.
- (11) Cooperate with any rescue attempt. Lie on the floor until told to rise.

### **B-20. Preparing the Family**

- a. Have your family affairs in order, including an up-to-date will, appropriate powers of attorney, and measures taken to ensure family financial security.
- b. Issues such as continuing the children's education, family relocation, and disposition of property should be discussed with family members.
- c. Your family should know that talking about military affiliation to non-DOD people may place you, or them, in danger.
- d. Don't be depressed if negotiation efforts appear to be taking a long time. Remember, your chances of survival actually increase with time.

### **B-21. Dealing with Your Captors**

- a. Do not aggravate them.
- b. Do not get into political or ideological discussions.
- c. Comply with instructions, but always maintain your dignity.
- d. Attempt to develop a positive relationship with them, but never praise the terrorist cause.
- e. Be proud of your heritage, government, and military association, but use discretion.
- f. Stay in Control:
  - (1) Maintain your composure as much as possible and recognize your fear. Your captors are probably as apprehensive as you, so your actions are important.
  - (2) Take mental notes of directions, times of transit, noises, and other factors to identify your location.
  - (3) Note the number, physical description, accents, habits, and rank structure of your captors. Anticipate isolation and efforts to disorient and confuse you.
  - (4) Try to mentally prepare yourself for the situation ahead. Stay mentally active.
- g. Keep Occupied:
  - (1) Exercise daily.
  - (2) Read anything and everything.
  - (3) Eat what is offered to you. You must maintain your strength.
  - (4) Maintain contact and where possible assist other captives.
- h. Interrogation:
  - (1) Take a simple, tenable position and stick to it.
  - (2) Be polite and keep your temper.
  - (3) Give short answers. Talk about nonessential matters, but be guarded when conversations turn to matters of substance.

(4) Don't be lulled by a captor's friendly approach. Remember, one terrorist may play the "good guy" and one the "bad guy." This is the most common technique.

(5) Ask to see U.S. Embassy personnel or representatives of an allied or neutral country.

(6) Resist exploitation by your captors.

(7) Avoid making a plea on your behalf.

i. During Rescue:

(1) Drop to the floor and be still. Avoid sudden moves. Wait for instruction.

(2) Once released, avoid derogatory comments about your captors; such remarks will only make things harder for those still held captive.

**Appendix C  
Personal Security Vulnerability Assessment (PSVA) Checklist**

**C-1. Introduction.**

The United States Army Criminal Investigation Command conducts Personal Security Vulnerability Assessments (PSVA) for General Officers and other Senior Officers in sensitive locations and/or sensitive positions. A PSVA will also be conducted for any personnel designated as a Level 1HRP.

**C-2. Purpose.**

The purpose of conducting a PSVA is to evaluate an individual's vulnerability to threat action. The PSVA addresses current security posture, identifies weaknesses where they exist and recommends corrective action.

**C-3. Overview.**

The primary areas analyzed in a PSVA are the work, home, and travel environments. Analysis of the work and home environments include an assessment of the general layout, security systems, communications, law enforcement support, and patterned behavior. Travel routes include analysis of communication, vehicle type, drivers training, route recon, and availability of safe havens.

**C-4. Home Security.**

a. House Location and Neighborhood

- (1) Are other US Nationals located in immediate area?
- (2) Is there evidence of high crime (e.g., frequent police patrols, overt security measures on local residences, etc.)
- (3) Is the dwelling located on a through-street or a cul-de-sac?
- (4) Is there off-street vehicular parking?
- (5) Are there apartment dwellings nearby? (If yes, is there off-street secure vehicular parking?)
- (6) Are phone/electrical lines overhead and exposed, or buried underground?
- (7) Is the home ever "swept" to uncover listening devices, phone traps, etc?
- (8) Are there physical barriers in the driveway to prohibit vehicles direct entry into the living area?
- (9) Is the principal's name/rank posted so as to identify the residence?
- (10) Are there multiple floors in the residence?
- (11) Are there above-ground level balconies?
- (12) Are there large trees near the dwelling affording possible entry to the house?
- (13) Is there a vehicular garage? If yes, is it attached to the house? If attached, is there an entryway from the garage to the house?
- (14) Are there large bushes near the house, which obscure windows/doors?
- (15) Is there any type of fencing marking the property lines? If yes, what type of fencing? If yes, are there gates or walkways/driveways? yes, can they be remotely controlled to allow ingress/egress?
- (16) Are there large trees or secure drainpipes near windows to make above ground entry to the house a possibility?

b. Apartment

- (1) Is it located on the ground floor? If not, on what level?
- (2) Is there more than one apartment per floor?
- (3) Does the apartment have an exterior-balcony? If yes, is the apartment easily accessible from outside (e.g., from an adjacent apartment balcony or fire escape)?
- (4) Are there elevators (freight, passenger); stairwells?
- (5) Are there exterior fire escapes?
- (6) If off-street parking is available, is it used? Are there multiple vehicle entrances/exists? Are they key controlled?

c. Lighting

- (1) Is there adequate lighting for:
  - (a) Sidewalks?
  - (b) Driveways?
  - (c) Entrances - house? garages?
  - (d) Perimeter of house?
  - (e) Yard area - front? back? side?
  - (f) Along the property line?
- (2) Is control of exterior lighting by manual switches in house/garage, photoelectric switches, trip wires, or other means?
- (3) Is exterior lighting protected by cage covers? Are they shatter proof covers?
- (4) Is there a system whereby occupants can activate all interior lighting with some type of portable duress switch?
- (5) Is the lighting protected by cage cover? covers? Are they shatter proof?

d. Entrances

- (1) Is door construction of solid wood hollow core? 24-gauge steel?
- (2) Are there glass panes in doors or adjacent to doors?
- (3) Do doors open inward or outward?
- (4) Locking device(s) of pintumbler, double cylinder, mortise, rime mount, or key in knob type?
- (5) If dead bolt locks are used, do they extend into door frames at least one inch? Do bolts have rotating steel rods in them? Are bolts protected by through-bolted escutcheon plates?
- (6) If Dutch doors are used, do they have dead bolts? Are dead bolts on each section, top and bottom?
- (7) Are chainlocks used on any doors? If yes, are they secured with screws into studs? Do they have integral locking devices?
- (8) Are sliding doors equipped with shattering glass; charlie bar, or other locking type devices? Are screws mounted-in tracks to prohibit lifting out of door panels?
- (9) Are locks changed if keys are lost or house staff is charged?
- (10) If there is a basement (cellar), is there an entrance into the house from this basement cellar? If yes, is that door of exterior grade construction? Does it have a dead bolt key operated locking device? Are its hinges secured?

e. Garage

- (1) Are there vehicle doors (overhead type)? Are there glass panels in door?
- (2) Does a locking bar protrude through the track? If yes, is a hole drilled through the bar at the end and a padlock inserted?
- (3) Is opening/closing controlled by electronic signal to a motorized opener? If yes, is the handscrew controlled by the principal only? If yes, is there an auxiliary switch in house/garage? If yes, can door be opened manually should the electricity be turned off?

f. Windows

- (1) Of what type construction are they (sliding, casement, awning, double hung, hopper, jalousie)?
- (2) Are the windows covered with security screens (through-bolted with exterior heads destroyed/welded to prevent removal)?
- (3) Are windows covered with security bars?
- (4) Are there locking devices on all windows?
- (5) Are windows made of or covered with shatterproof glass?
- (6) Are windows hung with sheer curtains (daytime) and lined curtains/drapes (nighttime)?
- (7) Are there devices in place, which make it possible to open windows only a few inches for ventilation (e.g., wooden blocks screwed into window tracks, and upper sash)?

g. Alarms

- (1) Are there adequate smoke/fire alarms installed?
- (2) Is there an IDS? Does it activate a local alarm, or an alarm at a police station or a contract monitoring station?
- (3) If there is an alarm, does it have window sensors, door sensors, monitor sensors, duress capability (stationary or portable?), or seismic sensors? (Around house and/or in driveway?)
- (4) Does the alarm system activate lights if it is activated?
- (5) Is there a backup power source for the alarm?
- (6) Is the alarm transmitted to an outside emergency via monitored telephone lines? Microwave lines?

## **FORSCOM Regulation 190-58**

- h. CCTV
  - (1) Is there CCTV coverage?
  - (2) Is it monitored in the house, at a police station, or at contract monitoring station?
- i. Guards
  - (1) Is the principal employing guards in his home? Are they local nationals? Have they been screened or had any type of background investigation?
  - (2) Are dogs employed? Are they trained attack dogs or family pets?
- j. Mail
  - (1) Is mail routed through the principal's office or come straight to the home?
  - (2) Is package delivery controlled?
- k. Safe haven
  - (1) Is one room designated as a safe haven?
  - (2) Does it have a reinforced door?
  - (3) Does it have a good lock?
  - (4) Is there communication equipment in the room?
  - (5) Is there a duress alarm in the room?
  - (6) Is there a fire extinguisher in the room?
  - (7) Are there first aid supplies in the room?
  - (8) Are there food and water provisions in the room?
  - (9) Is there emergency and/or portable lighting equipment in the room?
- l. Staff
  - (1) Does the principal/family/household staff verify authenticity of any telephone, plumbing, or repair people prior to permitting them entry?
  - (2) Is the household staff cleared by security check?
  - (3) Is household staff informed in advance of principal's travel plans, leisure time activities, etc?

### **C-5. Office Security**

- a. General Physical Measures
  - (1) Is entry controlled or open?
  - (2) Could entry to the building be restricted/controlled at all times?
  - (3) If controlled (restricted), is it done with guards or by mechanical means (e.g., key, card)?
  - (4) Could entry to the building be restricted/controlled at all times?
  - (5) Are there covered or concealed routes of approach?
  - (6) Are there ample fire escapes from the building?
  - (7) Are office grounds well lighted?
  - (8) Is there a waiting/reception room for visitors?
  - (9) Is there a peephole, interview grill, etc., for the purpose of screening visitors prior to admittance?
  - (10) Are restrooms kept locked? Are interior doors kept open except when in use? Have commode tank tops been secured?
  - (11) Have light switches (exterior and/or interior) been converted to key-type switches? Can lighting be activated by remote control?
  - (12) In OCONUS situations, is there a radio available and secured, to communicate with the protective services net established by the US embassies?
  - (13) Have mailboxes, trash bins, etc, located next to the building been moved?
  - (14) Are there security screens on windows?
  - (15) Does the principal have one unlisted phone number in his office to utilize for security business?
  - (16) Are there strategically located concrete barriers that prohibit direct approach and adjacent parking of vehicular traffic?
  - (17) Is the parking area fenced?
  - (18) Are gates to parking area controlled (electrical opening and closing)?
  - (19) Are there heavy draw drapes on all windows?
  - (20) Are windows shatterproof or protected with shatterproof coverings?
  - (21) Is furniture located away from walls/windows as much as is practical?
- b. General Procedural Measures
  - (1) Is the principal's itinerary and travel schedules appropriately safeguarded?
  - (2) Are the principal's activities stereotyped, or is randomness a planning consideration?

(3) Have essential elements of friendly information (EEFI) been developed to enhance the principal's security?

(4) Is the principal's parking space readily identifiable?

(5) Does the principal always park in the same spot?

(6) Is there adequate key control? Are locks changed if a key is lost or personnel are transferred? Are keys periodically inventoried?

(7) If weapons are stored in the building, are they stored IAW DOD 5100.7 or AR 190-11?

(8) Are all visitors escorted or otherwise controlled?

**c. Staff**

(1) Have guards been security screened?

(2) Is the office cleaned by outside personnel? Have they been security screened? If not, are they supervised during the time they are in the building?

(3) Do the principal and his staff understand techniques used by terrorists to collect intelligence?

(4) Are the principal and his staff generally familiar with the relationship between OPSEC and the principal's security?

(5) Have appropriate staff members been briefed regarding the operation and use of communication means with security forces?

**d. Safe Haven**

(1) Is one room designated as a safe haven?

(2) Does it have a reinforced door?

(3) Does it have a good lock?

(4) Is there communication equipment in the room?

(5) Is there a duress alarm in the room?

(6) Is there a fire extinguisher in the room?

(7) Are there first aid supplies in the room?

(8) Are there food and water provisions in the room?

(9) Is there emergency and/or portable lighting equipment in the room?

**e. Mail**

(1) Have mail handlers been taught to identify possible letter/package bombs and the proper procedure for dealing with them?

(2) Have mail slots been blocked or secured where appropriate?

**f. Electronic Security Systems**

(1) Is there an IDS?

(2) Does IDS activate a local alarm, or an alarm at a police station or a contract monitoring station?

(3) Is the alarm transmitted to an outside emergency via monitored telephone lines? Microwave lines?

(4) Is there a backup power source for the alarm?

(5) Are there portable duress alarms at building entry points?

(6) If there is an alarm, does it have: window sensors, door sensors, monitor sensors, duress capability (stationary or portable?), or seismic sensors?

(7) Does the alarm system activate lights if it is activated?

(8) Are there metal (airport type) detectors installed at restricted entrances?

(9) Is there CCTV coverage?

(10) Is CCTV monitored in the house, at a police station, or at contract monitoring station?

(11) Are there adequate smoke/fire alarms installed?

**C-6. Travel Security.**

**a. Private/Government Motor Vehicle**

(1) Is the gas tank kept at least half full?

(2) Is the car locked?

(3) Is the car always parked in the same place?

(4) Is the car marked so that identification of the principal is readily apparent?

(5) Is the car of local manufacture so as to blend into the environment?

(6) Does the car have local license plates?

(7) Is the car "hardened" in any way?

(8) Does the vehicle have

(a) Hood securing devices?

## **FORSCOM Regulation 190-58**

- (b) Tamper alarm?
  - (c) Gas fill lock?
  - (d) Bolt through end of the exhaust pipe?
  - (e) Mobile radio/telephone communications?
  - (f) Tool kit in trunk compartment?
  - (g) Fire extinguisher?
  - (h) Outside-rearview mirror on both sides?
- (9) Is the vehicle kept in top mechanical conditions?
- (10) Does the principal travel in uniform?
- (11) Does the principal travel-predictable routes and/or at predictable times?
- (12) Does a chauffeur do the driving? If yes, is he U. S. military or local National? Has he had evasive/defensive driving training?
- (13) Are the vehicle's windows kept closed?
- (14) Are location/routes to safe havens (e.g., police stations) known by chauffeur/principal?
- (15) Is the principal trained in evasive/defensive driving techniques?
- (16) If the principal is a HRP, is the vehicle equipped with one-way glass or curtains?
- (17) Is a suitable lead/chase vehicle employed?
- b. Public Conveyance (bus, train, plane, boat, etc.)
- (1) Does the principal travel in uniform?
- (2) Does the principal utilize well-lit, heavily used transit stations?
- (3) Does the principal avoid habitual travel patterns (i.e., using same bus or taxi)?
- (4) Does the principal travel alone?
- (5) When undertaking international travel does the principal avoid unfriendly countries and airports with poor ground security?
- (6) Does the principal sit near windows/doors?
- (7) Will the principal be especially vulnerable at any point during travel?
- (8) Does the principal allow his staff to make travel reservations/plans?
- (9) In the principal's travel/route/destination newsworthy?
- (10) Will scheduled and unscheduled stops (e.g., switchyards, and fuel stops) cause potential problems?
- (11) Can passenger manifests be secured in advance for screening?
- (12) Can reservations be made in the name of someone other than the principal?
- (13) Is it possible to run a name check on the operating crew?
- (14) In smaller crafts, is it possible to check identities of those in adjacent berths/seats/compartments?
- (15) Is the boat in an isolated area?
- (16) What communications are available?
- (17) Can the principal swim (in case of accident)?
- (18) If the principal remains aboard overnight, will guards be needed?
- (19) While underway (in a smaller craft), can a chase boat/plane be employed if desired?
- c. Helicopter
- (1) Can additional helicopters be utilized for chase/cover?
- (2) Can the landing zone (LZ) be secured to the extent necessary?
- (3) If nonmilitary, can the crew be screened to the extent necessary?
- (4) Can the principal's time on the ground be kept at a minimum as the situation dictates?
- (5) How public must the principal's departure/arrival be?
- d. Temporary Residence (Hotel, motel, etc.) during Travel
- (1) Is the lobby staffed on a 24-hour day?
- (2) Is there more than one elevator?
- (3) Is the principal's room located near an elevator, stairwell, fire escape, or freight elevator?
- (4) If there is a stairwell, are doors locked to prevent the access to selected floors?
- (5) Does the principal's room have a phone?
- (6) Is the principal's room exposed to adjacent buildings of the same or greater height?
- (7) Are there alternate entrances to the room?
- (8) Are there trash/storage/mail containers immediately adjacent to the principal's room?
- (9) Are there public latrines adjacent to the principal's room?
- (10) Are bellboys, house staff, etc., consulted as to directions to various points in the local area?
- (11) Does the principal invite newly acquired "friends" to his room?

(12) Does the principal receive mail at the temporary residence? If yes, is it necessary that it be received there? If yes, is the principal or residence staff briefed on techniques for identifying possible letter/parcel explosive devices?

(13) If a suspected mail bomb is identified, is local EOD support available to deal with it?

(14) Does the principal safeguard his passport and other valuable documents?

(15) Does the principal take care to mail personal post cards and letters himself? Does the principal ensure that no valuable information is printed on post cards?

(16) Does the principal insist on a room at the sixth-floor level or lower (firefighting equipment often cannot function above this level)?

(17) Is the principal aware of local emergency phone numbers (e.g., police, fire, ambulance, embassy, etc.)? Is the principal versed in the use of the local telephone system?

(18) Does the principal refuse unordered, unexpected packages?

(19) Does the principal employ portable locks/portable alarm systems when in temporary residences?

(20) Does the principal answer the phone using his name and rank?

(21) Does the principal draw the drapes in the room?

(22) Does the principal leave lights/radio on when not in -his room?

(23) Does the principal have his name/rank on the door of his temporary residence or in any other public area?

(24) Are the principal's arrival/visitation/departure/travel routes made available to local news media?

(25) Does the principal receive mail at the temporary residence reflecting his rank or position?

(26) Is the principal/staff aware of fire alarm/extinguisher/hose locations as well as procedures for operating them?

(27) Does the principal personally retain his room key at all times?

(28) Does the residence staff (e.g., chambermaid) have ready access to the principal's room?

### **C-7. Miscellaneous Security**

#### **a. Leisure Time Considerations**

(1) Does the principal/family members attend public events?

(2) Does the principal/family members attend any regular functions? (weekly, monthly, etc.)

(3) Does the principal/family members routinely attend highly publicized events?

(4) Is the presence of the principal/family members at public events a newsworthy item?

(5) Does the principal/family members stop (e.g., for food, gasoline, clothing) at regular intervals and frequently at the same location?

#### **b. Security of Children**

(1) Are children permitted to:

(a) Play alone?

(b) Play away from the residence?

(c) Travel unescorted?

(d) Participate in community events (e.g., sports, theatre, etc.)?

(2) Are school officials advised not to release the principal's children to other than family members and/or designated staff members, and only after -verifying identification?

(3) Do all family members know emergency phone numbers to call for assistance? Do they all carry enough funds to use pay telephones? In OCONUS situations, do they all know how to use the local telephone system?

(4) In OCONUS situations, do all family members know enough of the local language to seek help, police, and medical assistance?

(5) Does the members inform domestic help of planned absences, dates of return, etc.?

(6) Have all family members been fingerprinted for future identification purposes?

(7) Are keys to the residence controlled and restricted to family members?

(8) Is the residence under increased surveillance by local law enforcement and/or embassy staff when temporarily unoccupied?

(9) Do children notify parents when leaving home of expected time return, of route out and back and of phone number where they can be reached? Do they notify parents when a change of plans occurs? Do they communicate this information directly to a parent?