

**BY ORDER OF THE COMMANDER  
AIR FORCE RESERVE COMMAND**

**AIR FORCE INSTRUCTION 31-210**

**AIR FORCE RESERVE COMMAND  
Supplement 1**

**15 July 2000**

**Security**



**THE AIR FORCE ANTITERRORISM/FORCE  
PROTECTION (AT/FP) PROGRAM  
STANDARDS**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at: <http://afpubs.hq.af.mil>.

---

OPR: HQ AFRC/SFOF (Maj Mark S. Gunzelman) Certified by: HQ AFRC/SF (Col Francis M. Mun-  
gavin)

Pages: 11

Distribution: F

---

The OPR for this supplement is HQ AFRC/SFOF (Maj Mark S. Gunzelman). This supplement implements and extends guidance of Air Force Instruction (AFI) 31-210, 1 August 1999. The AFI is published word for word without editorial review. Air Force Reserve Command supplementary material is indicated by "(AFRC)" in boldface type. This supplement describes Air Force Reserve Command procedures to be used in conjunction with the basic instruction. Upon receipt of this supplement discard the Air Force basic

1.6. AFRC installation commanders are responsible for the AT/FP program at their respective installation.

1.8. (Added) Operations Security (OPSEC). The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary. OPSEC must be incorporated throughout the entire AT/FP program. Air Force OPSEC policy is located in AFI 10-1101, *Operations Security*.

1.9. (Added) Force Protection Performance Measures (FPPM). The Air Staff Security Forces/Force Protection Division (HQ USAF/XOFP) develops, implements, tracks, and reports the status of the Air Force's Force Protection Program (AF FPP). The purpose of the FPPMs is to mark milestones in the program and, as markers are met, FP measures will be discontinued and new ones established as needed. HQ USAF/XOFP identifies measures to be reported by message to the MAJCOM semi-annually during October and April. HQ AFRC/SF provides the FPPMs to the installation AT/FP Officer prior to the data call. The installation AT/FP officer collects and compiles the information required by the FPPM and provides it to HQ AFRC/SF by the 15th day of the reporting month.

3.1.1.2. (Added) At HQ AFRC, the Force Protection Board (FPB) serves as the primary body to advise the AFRC/CC/CV on AT/FP matters. The Director of Security Forces (AFRC/SF) chairs the FPB. As a minimum, the board consists of representatives from the following core functional areas: CE, DO, DOI,

DOZ, FM, LG, SC, SG, SF, AFOSI, and XP. In addition, associate members are requested to attend from the following functional areas: DP, HC, HO, IG, JA, PA, SE, SV, and RS.

3.1.11.1. Wing/Installation commanders are responsible for the implementation of AT/FP policies within their organizations. AFRC NAF/CCs will ensure AT/FP policies are established and adhered to relative to contingency and readiness operations.

3.2.3. AFRC Installation commanders must also develop a barrier plan for the protection of key facilities on their installation. The plan must address the specific location and placement of barriers, where they will be stored, and who is responsible to put them in place. This plan will be an annex to the Installation Security Plan (ISP) or the Installation AT/FP plan and should outline implementation procedures from THREATCON NORMAL through DELTA.

3.2.4. Installation commanders must budget for force protection requirements locally. If installations cannot fund force protection initiatives locally they forward them to HQ AFRC through their NAF as an unfunded requirement.

3.3.1. Within AFRC, AT/FP operational responsibility rests with the AFRC/CC/CV, NAF/CCs (during wartime planning), and down to installation and squadron commanders. Where AFRC facilities don't meet the criteria of an installation, the senior ranking person (military or civilian) has AT/FP operational responsibility.

3.3.4.1. Conduct AFRC installation-wide antiterrorism exercises (both operational and command post) semiannually, as a minimum. Conducting and evaluating these exercises together may fulfill this requirement. Use exercises to test and evaluate the installation's ability to respond to the local terrorist threat. Exercises will test a broad range of required THREATCON actions specified within the installation's local plans and may be combined with other base exercises such as a MARE, BROKEN ARROW, etc. As a minimum, conduct one of these exercises during a unit training assembly (UTA).

3.5.1.2. AFRC Installation commanders ensure a plan is developed for the protection of personnel and key facilities during increased THREATCONS.

3.6. HQ AFRC will establish a vulnerability assessment team (VAT) to conduct assessments of AFRC installations.

3.6.3. HQ AFRC/SF schedules JSIVA, AF and AFRC vulnerability assessments of AFRC installations through HQ USAF/XOFP. Coordinate schedule will with the HQ AFRC/IG Gatekeeper, the respective installation commander, and appropriate NAF/CC and SF.

3.6.4. HQ AFRC/SF is the lead agency to track lessons learned, trends, and best practices; and in coordination with the AFRC Force Protection Board, prioritize projects and program funding.

3.6.5. Vulnerability assessments (VA) are conducted on AFRC installations by the AFRC, AF, or JSIVA team every 3 years. VAs must ensure all tenant organizations (on the installation or remote but administratively attached) are integrated into the force protection plan and afforded the same level of FP support as AFRC units. AFRC vulnerability assessments are not required to physically assess every single activity on the installation, but instead must assess an appropriate number that will indicate a prudent level of FP is in place for the entire installation.

3.6.5.1. (Added) The AFRC VAT will plan to conduct assessments of all AFRC installations. Where this is not possible, coordinate with the JSIVA or HQ USAF/XOFP to provide assistance. **NOTE:** At installations where AFRC is the host, AFRC conducts an assessment of the entire installation. At installations

where AFRC is the tenant, the host unit's MAJCOM conducts an assessment of the entire installation to include AFRC assets.

3.6.5.2. (Added) AFRC VAT composition may vary based on the type installation being assessed. The assessment team consists of a team chief (SF lead), force protection specialist (two), structural/infrastructure engineer, civil engineer readiness specialist, medical readiness specialist, explosive ordnance disposal specialist, and a terrorist options specialist. Other functional experts may augment the team as needed. Augmentation depends on type of assessment required, the nature of the installation's mission, the terrorist threat level, and the THREATCON. Assessments may require expertise in linguistics, chemical/biological/radiological weapons effects, emerging AT/FP technology, information operations (IO), special warfare, or other specialties as determined by the commander or directed by HQ AFRC/SF. Regardless of team composition, the team must have expertise in these areas:

3.6.5.2.1. Physical Security.

3.6.5.2.2. Structural Engineering (Weapons Effect Specialist)

3.6.5.2.3. Operational Readiness.

3.6.5.2.4. Security Forces Operations.

3.6.5.2.5. Infrastructure Engineering.

3.6.5.2.6. Counterintelligence/Intelligence.

3.6.7. (Added) Installation commanders must make every attempt to correct AT/FP vulnerabilities identified during DoD Standards 6 and 14 vulnerability assessments; especially those that are procedural or low cost and would improve the AT/FP posture. Conversely, high cost improvements must be reviewed in context with threat and risk assessment, planned for, and programmed.

3.8.2.1. AFRC Installation commanders maintain close liaison with the AFOSI office servicing their respective installations.

3.9.2. Use the Demography, Symbolism, History, Accessibility, Recognizability, Population, and Proximity (DSHARPP) methodology (attachment 6) to determine the risk associated with the threat to the installation.

3.9.3. AFRC Installation commanders will ensure terrorist threat assessments for their area of responsibility are incorporated in the risk assessment development process and may be included as a separate annex to the installation security plan (ISP).

3.10.3. All AFRC installations will establish and maintain an active Threat Working Group (TWG) which will meet, as a minimum, on a monthly basis and as situations warrant due to increased threat. Installation TWGs are strongly encouraged to invite their local civilian law enforcement agencies that have legal jurisdiction over their installation. AFRC units which are tenant on active duty bases will actively seek membership with the host's TWG. The installation TWG will conduct a review of future deployments of personnel and aircraft to ensure proper AT/FP training and security measures are being implemented. Additionally, installation TWGs should review and analyze local threat data. All AFRC units review the HQ AFRC TWG weekly deployment advisory message to ensure compliance with AT/FP measures.

3.10.3.1. (Added) HQ AFRC Threat Working Group (TWG) Charter. HQ AFRC/DOI chairs the TWG. Primary members are DOOM, SFOF, and AFOSI. Other staff offices may participate as required. The TWG meets as often as required but not less than once weekly.

3.12.2. AFRC Installation commanders decide when to go to higher THREATCONs based on local conditions. Downward directed THREATCON changes for AFRC units will come from or through AFRC/CC. Tenants on AFRC bases should coordinate with owning MAJCOM/service THREATCON changes and seek concurrence from the host prior to implementing the THREATCON. AFRC Installation commanders consider the request, determine local threats, and make a base-wide determination. In those instances where local threats are absent, commanders seek clarification from AFRC prior to increasing THREATCONs. There will only be one THREATCON on AFRC bases, with final determination made by the installation commander.

3.12.3. All AFRC installations will immediately notify the AFRC command post upon any change in the local THREATCON.

3.13.1.4. Installations will develop and implement written local RAMs. To be effective, use RAMs in THREATCONs Normal to Delta. As a minimum, use the RAMs contained within AFI 31-210, attachment 3. Fifty-one security measures are listed for THREATCON Alpha through Delta with one measure in each THREATCON to be determined. Locally devised measures above and beyond THREATCON Charlie may be used. Locally developed measures will follow the format provided in AFI 31-210, attachment 3. In other words, list the DoD measure and supplement with additional local measures. For example, AFI 31-210, attachment 3, paragraph A3.2.2.1 depicts DoD Measure 1. Paragraphs A3.2.2.1.1 and A3.2.2.1.2 are Air Force added supplemental measures.

3.14. Installation commanders will ensure physical security vulnerability assessments are conducted every 3 years and reports forwarded to HQ AFRC/SF. Refer to DoDO-2000-12H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, (Appendix C, Physical Security Survey Instrument) for guidance on how to conduct a physical security vulnerability assessment.

3.14.2. The Installation Chief of Security Forces is the OPR for conducting physical security vulnerability assessments within AFRC. Include off-site activities (outside-the-fence) as part of the assessment. Conduct assessments every 3 years or when significant changes occur. Complete initial Standard 14 assessments by December 2000. As a minimum, assessment team composition includes Security Forces (lead), AFOSI, Civil Engineering, Intelligence, Medical, and Communications. A qualified representative from the wing Information Protection Office conducts the communications portion of the physical security vulnerability assessment. Results of the Information Protection Assessment Program review conducted according to AFI 33-230, *Information Protection Assessment and Assistance Program*, will supplement the physical security vulnerability assessment. Use the JSIVA checklist, the checklist provided as an attachment to DoDO 2000.12-H, and AFOSI Pamphlet 71-123, to accomplish the assessments. Classify physical security assessment vulnerability reports pursuant to the JSIVA Security Classification Guide, Jan 2000. Forward a courtesy copy of the completed DoD Standard 14 assessment to HQ AFRC/SF within 90 days after the assessment.

3.15.3. Recommend installation commanders use the Joint Chiefs of Staff J-34 Antiterrorism Force Protection Installation Planning Template (interactive CD-ROM) when creating or updating an installation AT/FP Plan; extract data produced by the CD-ROM when writing the AT/FP Plan. When the Installation Security Plan is completed per AFRC Supplement to 31-101, *Installation Security Program*, chapter 4 (Planning Security Operations) it becomes a combined overarching AT/FP Plan.

3.15.3.1. (Added) Recommend installation commanders use the Joint Chiefs of Staff J-34 Weapons of Mass Destruction Appendix (interactive CD-ROM) to the Antiterrorism Force Protection Installation Planning Template when creating the response actions of the Installation Security Plan.

3.16.1. Local command authorities exercise all portions of their AT/FP plans semi-annually. Involve local off-base agencies to the greatest extent possible and encompass duty and non-duty hours. Also include all tenant activities and/or DoD elements and personnel for whom the commander has force protection responsibility.

3.17. Commanders at all levels routinely (or when the Terrorist Threat Level changes) review the effectiveness of day-to-day physical security measures under the existing THREATCON posture. As a minimum, consider access control, patterns of population concentrations for both work and social purposes, and sensitive areas that may be lucrative targets for terrorists and criminals.

3.19.2. AFRC Installation commanders will ensure SV and LGC coordinate with the installation AT/FP officer, AFOSI, and SF to ensure threat assessments are conducted of all off-base lodging facilities being used by personnel during TDYs or UTAs.

3.20.2. All Command, Control, Communications, Computers and Intelligence (C4I), headquarters, and lodging facility projects, whether new construction or major renovation, will be reviewed by HQ AFRC/SF and installation SF personnel during the initial design process to ensure force protection considerations are properly addressed. Consideration should be given to constructing a "Safe Haven" location for installation commanders in their office to be used during duress situations. Refer to the Interim Department of Defense Antiterrorism/Force Protection Construction Standard dated 16 December 1999 and DoDO-2000.12H, chapter 10.

3.21. The MAJCOM and installation TWG conducts these assessments according to paragraph 3.10.3.

3.21.2. Refer to the Interim Department of Defense Antiterrorism/Force Protection Construction Standard dated 16 December 1999 and DoDO-2000.12H to aid in developing AT/FP factors.

3.23.4. Installation placement of the AT/FP Officer and alternate at AFRC field activities is at the commander's discretion; however, commanders should consider collocating the AT/FP Officer and alternate with force protection or program protection personnel to ensure effective implementation across organizational and functional lines. The person appointed may be an officer, NCO, DoD civilian, or for those installation/sites with contracted security, a DoD contractor. Grade criteria for the AT/FP Officer and alternate should generally target military O-2/3, E-6, or DoD civilian GS-9. Based on mission need the installation/site commander may waive target grades. Once the AT/FP Officer and alternate have been designated, forward a courtesy copy of the appointment letter containing the person's name, SSN, security clearance, duty phone number and e-mail address to HQ AFRC/SF. Update appointment letters as changes occur.

3.23.4.1. Commanders are strongly encouraged to appoint in writing individuals who have experience, education, training, etc. to serve as their AT/FP Officer and alternate. Those appointed installation AT/FP Officers should attend Level II training within 90 days of appointment. If the installation commander identifies an AT/FP Officer/alternate who has past experience, education and training, the commander may exempt them from Level II training. This exemption needs to be done in writing and identified in the AT/FP appointment letter.

3.24.7. Unit training managers will annotate dates of completion of AT/FP Level 1 Training in PC-III when the PC-III system has been updated to accept this information. Unit commanders of personnel deploying to overseas locations will ensure annotation of this training on the individual's travel orders and/or instruct them to hand-carry a copy of the PC-III print-out which indicates training has been completed.

3.24.8.1. Commanders will develop written procedures to ensure proof of Level I training is part of the TDY order/leave authenticating process. Personnel who have not completed Level I AT/FP training with special emphasis on AOR-specific threat and medical threats will not be issued orders for overseas travel (deployed, TDY or leave). The Joint Staff Guide 5260 is available via GCCS on the J-34 Combating Terrorism web site <http://nmcc20a.nmcc.smil.mil/~dj3cleap/j34pubsdocs/j34/pubsdoc.html>. Local reproduction is authorized.

3.24.8.4. Commanders and directorate heads must ensure their personnel receive annual force protection training. The DoD AT/FP video "You May Be the Target" is the tool used to conduct the annual force protection training. Use this IP address <http://dodimagery.afis.osd.mil> to order the video. Document force protection training in the same manner as other ancillary training. Training documentation is subject for review during vulnerability assessments conducted pursuant to DoD Standards 6 and 14.

3.24.9. Units needing Level II training schedule the requirement with HQ AFRC/SFOF. Personnel selected to attend the Level II course must be prioritized as follows: installation AT/FP Officer and alternate, key leadership assigned to UTCs, and other specialties on the installation key to successful UTC deployment; i.e., combat logistics, communications, prime beef, medical personnel and other unique teams. Submit prioritized Level II training requests to HQ AFRC/SFOF under wing commander or equivalent signature. Requests must include full name, rank/grade, SSN, security clearance, and duty phone to facilitate the request.

3.24.9.1. All AFRC AT/FP Level II Mobile Training Team (MTT) instructors will be certified by HQ AFRC/SF prior to instructing any AFRC classes. HQ AFRC/SFOF establishes an AT/FP Level II instructor list of certified instructors. The AFRC AT/FP Level II MTT instructor list is made up of lead instructors and support instructors. A minimum of one lead instructor must be present to control the course of instruction during all AFRC AT/FP Level II classes. Lead instructors are graduates from the Antiterrorism Instructor Qualification Course (AIQC). Support instructors are graduates of an AT/FP Level II course and have functional expertise in the AT/FP subject matter.

3.24.10. HQ AFRC/SF provides Level III training during the AFRC squadron commander orientation course taught at Robins AFB GA.

3.25.3. Procedures prohibit the issuance of orders for overseas travel (deployed, PCS, TDY or leave) for those personnel who have not received Level I AT/FP training with special emphasis on AOR-specific threat and medical threats.

3.26.4. Executive officers, executive secretaries, and others responsible for accomplishing itineraries for general officers, AFRC installation commanders, and DAF civilian equivalents are responsible for marking travel itineraries For Official Use Only (FOUO) or classifying the itineraries confidential when required. The itinerary classified by line shall read:

**Derived From: AFI 31-210, 1 Aug 99**

**Declassify On: Completion of Trip**

3.28. Strongly encourage Terrorism Incident Response Plans be added to the installation security plan or the installation AT/FP plan.

3.28.3. As a part of the response plan, commanders are encouraged to develop a set of recognizable alarms for potential emergencies. Each alarm should have its own set of reactions and a means to immediately sound the alarm. Commanders should conduct frequent drills to familiarize all personnel with individual responsibilities during a potential emergency.

3.30.3. Installation commanders consult with their servicing AFOSI detachment if executive protection and protective services are needed.

3.31.1. Installation commanders task the appropriate intelligence/counterintelligence organization under their command to collect, analyze, and disseminate terrorist threat information pertaining to the potential terrorist use of WMD. Commanders at all levels ensure personnel under their command properly report information on events or situations that could pose a threat to the security of DoD personnel and resources.

3.32.1. As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and NBC staff elements. The entire range of potential terrorist WMD use should be considered when conducting assessments. Threats from commercial chemical, biological, nuclear, and radiological sources should be included as well as traditional military agents. Examples of vulnerabilities include:

3.32.1.1. Individual protective equipment/clothing.

3.32.1.2. Collective protection equipment and facilities,

3.32.1.3. Medical response and emergency services capability.

3.32.1.4. raining of personnel.

3.32.1.5. Physical security and protective barriers.

3.32.1.6. Facility design and construction.

3.32.1.7. Early warning and detection.

3.32.1.8. Alarms and attack warning.

3.32.1.9. Threat intelligence.

3.32.1.10. Preventive medicine and vaccination programs,

3.32.1.11. Sustainment operations and follow on support,

3.32.1.12. Storage of bulk hazardous material,

3.32.1.13. Explosive ordnance disposal response capability/availability.

3.32.1.14. Food and water sources.

3.33.2.1. Send reports to HQ AFRC/SFO who, in turn, sends the information to AFSFC/SFP.

3.33.2.7. (Added) As a part of the overall installation/site AT/FP plan, commanders should address the WMD threat and exercise the WMD part of the plan to determine its effectiveness in mitigating the effects of an attack. In addition to providing crisis action and consequence management procedures, planning should include pre-attack measures and consideration for collateral damage a WMD may have on adjacent facilities and surrounding communities. Plans should provide sufficient detail to permit organizations to rapidly recognize and respond to any terrorist event using WMD. Attachment 6 provides additional crisis action planning considerations that should be included in addressing terrorist use of WMD.

**Attachment 6**

**DEMOGRAPHY, SYMBOLISM, HISTORY, ACCESSIBILITY, RECOGNIZABILITY, POPULATION, AND PROXIMITY (DSHARPP) MATRIX EXPLANATION**

**A6.1.** The purpose of the DSHARPP matrix is to analyze likely terrorist targets. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (for example, "attractiveness" to enemy, potential psychological effect on community, etc.) of potential targets. This document provides an example of how to use DSHARPP.

**A6.2.** After developing a list of potential targets, use the DSHARPP selection factors to assist in further refining your assessment by determining the most likely (i.e., efficient, effective, and plausible) method of attack and identifying vulnerabilities to that type of attack. After the DSHARPP values for each target or component are assigned, the sum of the values indicate the highest value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

**A6.3. Demography**

**A6.3.1.** Demography focuses mainly on the threat to personnel and asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. Therefore, when assessing points in this area, determine whether or not the group(s) have a history of or are predicted to target:

A6.3.1.1. Military members.

A6.3.1.2. Family members (US citizens in general).

A6.3.1.3. Civilian employees of the US government (include local nationals).

A6.3.1.4. Senior officers or other high-risk personnel.

**A6.3.2.** Assess points to the target facility (scale of 1-5; 5 being worst) in this area based upon the MO of the group in targeting specific groups, and the potential for the target to be attacked based on its housing personnel of that particular group.

<b>CRITERIA</b>	<b>SCALE</b>
Facility routinely contains substantial numbers of personnel known to be targeted by the enemy	5
Contains known target group, but rarely in large concentrations	3-4
Little target value based on demographics of occupants	1-2

**A6.4. Symbolism.** A consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of US military, religious group disfavored by the enemy, government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

<b>CRITERIA</b>	<b>SCALE</b>
-----------------	--------------

High profile, direct symbol of target group or Ideology	5
Low profile, direct symbol of target group or ideology	3-4
Low profile and/or obscure symbol of target group or Ideology	1-2

**A6.5. History.** Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.

CRITERIA	SCALE
Strong history of attacking this type of target	5
History of attacking this type of target, but none in the immediate past	3-4
Little to no history of attacking this type of target	1-2

**A6.6. Accessibility.** A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period. The four basic stages to consider, when assessing accessibility are:

**A6.6.1.** Infiltration from the staging base to the target area

**A6.6.2.** Movement from the point of entry to the target or objective

**A6.6.3.** Movement to the target's critical element

**A6.6.4.** Exfiltration

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed	5
Inside Perimeter fence, climbing or lowering required	3-4
Not accessible or inaccessible without extreme difficulty	1-2

**A6.7. Recognizability.** A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility (yours and the enemy's). Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must be considered.

**A6.7.1.** Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

<b>CRITERIA</b>	<b>SCALE</b>
Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition	5
Target is easily recognizable at small-arms range and requires a small amount of training for recognition	4
Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition	2-3
Target cannot be recognized under any conditions -- except by experts	1

**A6.8.** Population. What is the population relative to other potential targets? Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

<b>CRITERIA</b>	<b>SCALE</b>
Densely populated; prone to frequent crowds	4-5
Relatively large numbers of people, but not in close proximity (That is, spread out and hard to reach in a single attack)	3
Sparsely populated; prone to having small groups or individuals	1-2

**A6.9.** Proximity. Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection? (for example, near national monuments, protected/religious symbols, etc., that the enemy hold in high regard)

<b>CRITERIA</b>	<b>SCALE</b>
Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel	5
Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction	3-4

Target is in close proximity; serious injury/damage or death/total destruction of protected personnel/facilities likely	1-2
---	-----

**NOTE:** It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

**A6.10.** Add the scores across the rows to produce the DSHARPP score for that particular target to that mode of attack. The costs for compensatory measures developed to mitigate/eliminate the vulnerabilities identified is placed in the FPIM where the row for the type of facility (target) and the column for the corresponding DSHARPP score intersect.

JAMES E. SHERRARD III, Maj Gen, USAF  
Commander