BY ORDER OF THE COMMANDER SHAW AFB

SHAW AIR FORCE BASE INSTRUCTION 31-102

6 DECEMBER 2012

Security

INTEGRATED DEFENSE (ID) AWARENESS TRAINING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: Access to this publication is restricted. This publication may be released to government employees with access to the restricted website.

OPR: 20 SFS/S5-A

Certified by: 20 SFS/CC (Lt Col Mark R. Walsh)

Supersedes: SHAWAFBPAM 31-102, 11 August 2004

Pages: 27

This instruction implements Air Force Instruction 31-101 ACC Supplement, *Integrated Defense*, Attachment 15, *Integrated Defense (ID) Awareness Training*. This instruction serves as the localized plan for conducting PHASE I and II training of the Air Combat Command (ACC) Integrated Defense (ID) Awareness Training Program. Additionally, it will acquaint you with the internal security measures used in Shaw AFB restricted areas, entry requirements, and most importantly, the part YOU play in protecting our nation's valuable resources. If you have any questions, please ask your unit Flightline Protection Program Monitor, Security Manager, or call the base Flightline Protection Program Manager at extension 5-3629. For extensive guidance on security matters refer to AFI 31-101, *Integrated Defense*, ACC Supplement 1 or SAFB Plan 31-101, *Integrated Base Defense Plan* (IBDP). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://my.af.mil/afrims/afrims/afrims/rims.cfm**. Contact supporting records managers as required. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s to 20 SFS/S5-A, 524 Nelson Ave., Shaw AFB, SC 29152-5051; route through your appropriate functional chain of command.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include the conversion from obsolete AFI 31-101, *Installation Security*, 1 Mar 03, requirements to AFI 31-101, *Integrated Defense,* 8 Oct 09, requirements.

INTEGRATED DEFENSE (ID) AWARENESS TRAINING

1. Overview. This attachment serves as the standardized lesson plan for Phase I of the Air Combat Command (ACC) Integrated Defense Awareness Training program. Security Forces and unit-appointed Phase I and II training officials must supplement this attachment to meet unit needs. Use AFI 31-101, *Integrated Defense*, ACC Supplement, AFI 10-245, *Antiterrorism (AT)*, and the local Installation Defense Plan (IDP) when developing supplemental information. The supplement should include, but is not limited to, specific restricted area entry controls, methods individuals may use to gain unauthorized entry, and a description of the local threat. Blank spaces throughout this attachment should be supplemented to meet individual base situations.

2. Objective. The objective of ID awareness training is to instill in every Air Force member a sense of responsibility for securing protection level resources. This sense of responsibility enables us to react quickly and correctly to threats against protection level resources. Commanders expect personnel receiving integrated defense awareness training to attain the necessary skills to apply proper ID techniques within their area of responsibility. For example, an administrative specialist who does not work either on a flightline or in a restricted area does not need the same depth of understanding as an aircraft maintenance specialist whose place of duty is within a restricted area.

2.1. Before granting unescorted entry to a restricted area, personnel must pass a standard physical security awareness test administered as part of Phase I training. Minimum passing score must be 80 percent. Remedial training for individuals not attaining a score of 80 percent will be provided during initial training. Units may use the Phase I Security Awareness test located at Attachment 3 to meet this requirement.

3. Concept. In accordance with Air Force Policy Directive (AFPD) 31-1, *Integrated Defense*, Security Forces (SF) is the enterprise leader for ID operations; however, it is not an entirely "SF" program. Capabilities-based ID is a fundamental battle competency for all Airmen, whether garrison or deployed, and requires active participation by all to ensure success. Security of assets that defend our nation, people and equipment, is an inherent responsibility of command and requires the effort of every Airman regardless of AF specialty, rank or position. This active participation truly integrates defense efforts.

4. Phase 1 Orientation Training.

4.1. Introduction. Welcome to Shaw Air Force. In keeping with Air Force policy regarding ID education and motivation, the HQ ACC/A7S staff and the 20th Security Forces Squadron designed the following orientation not only to introduce you to the ACC Integrated Defense Awareness Training Program, but also to point out your individual responsibilities. This training is in compliance with the provisions of AFI 31-101 and AFI 31-101, ACC Sup 1. To understand these responsibilities, we will first discuss the general concept of the program and security threats confronting us. We will then examine the security reporting and alerting system, how to control entry, individual responsibilities, and finally, key installation security documents.

4.2. Concept of Integrated Defense Program. Per AFPD 31-1, ID is "the application of active and passive defense measures, employed across the legally-defined ground dimension of the operational environment, to mitigate potential risks and defeat adversary threats to Air

Force operations." ID is planned and executed based on the estimated threat (or combination of threats) and operating environment and approved by the installation commander.

4.3. Purpose.

4.3.1. Many of the policies and procedures that governed the defense of our warfighting assets revolved around our Cold War mission. However, since the end of the Cold War, the threats to our people and resources have changed significantly, but our policies and procedures to defend our war fighting resources have remained the same. Furthermore, the lines between peacetime and wartime are blurred by the ever-present threat of terrorism and as a result, a change in approach to securing our personnel and resources is necessary. ID bridges the gap between peacetime and wartime actions to secure the force, as well as provide all personnel with the necessary tools to determine how to secure their assets. Just as each installation has its own unique mission and challenges, each commander/manager must be capable of applying tailored, threat-based security planning after thorough analysis of the operational environment and available resources.

4.3.2. The shift to ID requires a significant change of perspective in two central areas. The first change is from resource-based defense posture to a risk-based defense posture. The second change is from compliance-based operations to effects-based operations. Previous guidance was "directive-centric" and executed through compliance with specific regulations, measures and standards without considerations to their effectiveness. Responsibility was obtained from guidance or instructions, and success was measured by how well checklists were followed. The shift to risk- and effects-based operations focuses on deterring and defeating threats with limited personnel and resources. Previous guidance told us "what" to defend and "how" to defend it without consideration of the threat, vulnerabilities and operating environment unique to each installation.

4.4. System. ID occurs during all facets of AF operations, from routine peacetime activities through crisis development and contingency operations. During peacetime activities, ID efforts focus on criminal activity and pre-operational terrorist planning that may affect our people, resources, and readiness. During contingency operations, ID focuses on Level I, II, and III threats that may affect our ability to execute AF missions. This "continuum" makes no distinction between Continental United States (CONUS) and Outside Continental United States (OCONUS), garrison or deployed locations. What does change is the threat to our personnel, resources and operating environment. These threats can be just as high at CONUS installations as they are at deployed locations.

4.5. Goal. The goal of ID is to neutralize security threats throughout the Base Boundary (BB) in order to ensure unhindered AF operations. Through ID, commanders must: minimize mission degradation from threat activity within the BB and coordinate necessary security operations support within the Base Security Zone (BSZ) when the BSZ is not congruent with the BB; minimize loss of life and injury from threat activity; and protect government property and personnel from hostile and criminal acts. The end state is to create a flexible, responsive ID operation within varying threat environments.

4.6. The Protection Level (PL) System. The PL system determines the level of security dedicated to resources based on programmed manpower. This system recognizes that Installation Commanders must accept varying degrees of risk to establish baseline security standards. Based on the local threats and availability of limited resources, installation

commanders use the Integrated Defense Risk Management Process (IDRMP) to determine optimum resources and tactics, techniques, and procedures (TTP) to effectively counter threats to PL 2 and PL 3 power projection assets and PL 4 mission support assets.

4.6.1. Factors of Protection Level Designation. The assigned level reflects:

4.6.1.1. The importance of the resource to the overall United States warfighting capability.

4.6.1.2. The known or postulated threat to the resource.

4.6.1.3. The alert status.

4.6.1.4. The existence of local paramilitary groups who have the capability and intent to damage or destroy the resource.

4.6.1.5. The political significance to the United States (US).

4.6.1.6. The number of operational resources available in the United States Air Force (USAF).

4.6.1.7. The location of the resource in relation to probable threat or damage.

4.7. Protection Level Assignments.

4.7.1. Protection Level 1: AF power projection assets for which the loss, theft, destruction, misuse or compromise would result in great harm to the strategic capability of the US. Limited funding dictates our most important national defense assets receive the greater share of available SF resources. This level of security must result in the greatest possible deterrence against hostile acts. Failing the ability to deter, defensive measures will provide maximum means to detect, and defeat of a hostile force before it is able to seize, damage, or destroy resources. Owners/users of PL 1 resources must be actively involved in security of their assets. Response is provided by SF. Currently, there are no PL 1 resources permanently assigned to Shaw AFB. Examples of PL 1 resources include nuclear weapons and/or critical components, Command, Control, Communications, and Computer Systems critical to the success of active nuclear missions, and designated critical space and launch resources.

4.7.1.1. We must take all threats against our PL resources seriously. Our mission is weakened as long as our base is vulnerable to clandestine activities such as terrorism, espionage, and sabotage. We can eliminate this weakness only by YOUR active participation in our security system. To accomplish this, you must be knowledgeable of the local threat.

4.7.1.2. The most visible peacetime threat to resources located on Shaw AFB stems from the conduct of vandalism and civil criminal activity resulting in theft, damage, or destruction of resources. Terrorism is considered to be the most significant and unpredictable threat to Shaw AFB resources. Although installations in CONUS have for the most part, been spared from direct terrorist activity, the threat **cannot be overlooked**. The events of September 11, 2001 proved the unpredictability of the threat and that vulnerabilities do exist for all CONUS military and civilian facilities. The peacetime threat of sabotage comes from domestic political activists like the Plowshares, who have a proven record of anti-US military destructive activity.

4.7.1.3. A threat possibly overlooked may come from someone you work with day-to-day. The expression, "it must have been an inside job," is a reasonable description of this type of threat. This threat can manifest itself at anytime. For example, the threat could possibly come from an enemy agent who has infiltrated our ranks or from a disgruntled coworker who purposely damages Air Force resources. Our best defense against this type of threat is increasing our awareness of its potential existence.

4.7.1.4. Individual Responsibilities.

4.7.1.4.1. You are about to be issued an USAF Restricted Area Badge (RAB). This badge will authorize you unescorted entry into Shaw AFB restricted areas containing PL 3 resources. This authorization also carries certain security responsibilities that are inherent to your job. While within a restricted area, you must attach your badge to your outermost garment **above the waist** and displayed with the picture facing out at all times. ACC has made one exception to this rule; aircraft maintenance personnel doing intake/exhaust inspections. During these times, you may conceal your badge, however, it must be displayed immediately upon completion of the work. Personnel performing functions around paint or hazardous chemicals that could damage the badge should use common sense in protecting it. Personnel not displaying a restricted area badge will be challenged by SF or others working in the area to verify their authorization to be in the area. You should always enter and exit restricted areas at the entry control point unless otherwise coordinated.

4.7.1.4.2. When you depart the restricted area, remove your badge from your outermost garment and secure the badge out of sight. A buttoned shirt pocket is the best place.

4.7.1.4.3. Should you lose your badge, report the loss to your security manager immediately. You and your security manager must make every effort to find your badge and investigate its loss before a new badge can be issued. ***NOTE:*** Escorting personnel who have unescorted entry and are not in possession of their RAB is not authorized. The individual must retrieve their badge prior to entering the area.

4.7.1.5. Owner/User Responsibilities. Owner/users, also known as supporting force personnel, are defined as those personnel to whom custody of the aircraft has passed. These personnel will establish and enforce temporary restricted areas around aircraft removed from permanent restricted areas. These temporary areas will be marked with restricted area signs, rope, and stanchions. For aircraft located in the wash rack, maintenance hangars, or paint barns, a 4 x 6 inches wide painted red line, ropes and restricted areas signs may be used to delineate these temporary restricted area boundaries. Hangars containing PL 3 aircraft (i.e., 1200/1614) become restricted areas when aircraft are present and RABs must be displayed IAW paragraph 6.1.

4.7.1.6. Identification of Personnel Within Restricted Areas.

4.7.1.6.1. While within any restricted area, you are responsible for determining whether personnel known or unknown to you are authorized to be in the area. Know the proper area number on the badge for entry into restricted area. When

checking someone's restricted area badge, look it over carefully and make certain the number for the area is not blotted out. Know the locally devised authentication codes for your restricted area badge. If you find any portion of the badge to be incorrect, contact the Security Forces and have the individual checked out. Don't be quick to accept individual's claims or excuses.

4.7.1.6.2. BE ALERT for unauthorized personnel in the area, or people/vehicles entering/exiting through other than established entry/exit points. KNOW what is going on around you at all times. When you approach a person, look for the restricted area badge. If the person has a proper badge and you recognize them, resume your normal duties. If the person has a badge, but is not recognized as a coworker, or is acting suspicious, check them out further and determine if they are authorized to be in the area.

4.7.2. Protection Level 2: AF power projection assets for which the loss, theft, destruction, misuse, or compromise would cause significant harm to the warfighting capability of the US. For example, a CONUS Satellite Communication (SATCOM) facility supporting one wing and part of a network capable of performing the same mission without loss of mission support, may be designated a PL 2 asset. In comparison, a SATCOM facility located OCONUS with no redundancy, and supporting a joint theater, may be designated PL 1. This level of security must result in significant deterrence against hostile acts. Failing the ability to deter, defensive measures will ensure a significant probability to detect, and defeat a hostile force before it is able to seize, damage, or destroy resources. Owners/users of PL 2 resources must be actively involved in security of their assets. Response is provided by SF. Currently, there are no PL 2 resources permanently assigned to Shaw AFB. Examples of PL 2 resources include non-nuclear alert forces, expensive, few in number, or one of a kind systems, and vital computer facilities and equipment.

4.7.3. Protection Level 3: AF power projection assets for which the loss, theft, destruction, misuse, or compromise would damage US warfighting capability. This level of security must result in a reasonable degree of deterrence against hostile acts. Failing the ability to deter, defensive measures must be able to delay a hostile force and limit damage to resources. Owners/users of PL 3 resources must be actively involved in security of their assets. Response is provided by SF. Examples of PL 3 resources are weapons systems capable of being on alert status, selected command, control and communications facilities, systems and equipment, and intelligence-gathering systems not critical to US operational capability.

4.7.3.1. The Protection Level 3 resources on the installation are:

4.7.3.1.1. F-16 Mass Parking Areas.

4.7.3.1.2. Wing Command Post.

4.7.4. Protection Level 4: Assign PL 4 to AF mission support assets which do not meet the definitions of PL 1, 2, or 3 resources as discussed in the preceding paragraphs, but for which the loss, theft, destruction, misuse, or compromise would adversely affect the operational capability of the Air Force. Protection Level 4 resources are contained in controlled areas with owners/users being responsible for security. Response is provided

by SF. Examples of PL 4 resources include facilities storing arms, ammunition and explosives, petroleum, oils and lubricants and liquid oxygen storage areas, warehouses storing aircraft or weapons systems spare parts and AF pharmacies and medical logistics vaults.

4.8. Threat Types.

4.8.1. Traditional and non-traditional ground threats could include, but are not limited to, crime, espionage, hostile surveillance, sabotage, subversion, civil unrest, terrorism, irregular or unconventional warfare, and conventional warfare. Furthermore, criminal activity such as pilferage of critical items, information theft, and violent crimes may also have an impact on air operations. At higher levels of conflict, the threat may include chemical, biological, radiological, nuclear and high-yield explosive weapons, as well as air-to-surface and surface-to-surface attacks with conventional weapons. The adversary's acquisition of technologically advanced equipment, such as portable surface-to-air missiles, guided mortar munitions and night vision devices increases the difficulty to detect or neutralize threats to air bases. This range of potential adversaries includes the three traditional levels of threats described below, as outlined in Joint Publication (JP) 3-10, *Joint Security Operations in Theater*. These threats may occur simultaneously and are not necessarily dependent on one another.

4.8.1.1. Level I Threats. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion. Enemy activity and individual terrorist attacks may include random or directed killing of military and civilian personnel, kidnapping, and/or guiding special-purpose individuals or teams to targets. The most effective way to defeat the Level I threat is to disrupt the planning process through the use of sound AT techniques before an attack occurs. Base defense forces must be capable of detecting and defeating Level I threats.

4.8.1.2. Level II Threats. Level II threats include small-scale, irregular forces conducting unconventional warfare that can pose serious threats to military forces and civilians. These attacks can cause significant disruptions to military operations as well as the orderly conduct of local government and services. Base defense forces must be capable of disrupting or delaying Level II threats until the arrival of response forces. These response forces are normally military police units assigned to the Joint Security Area.

4.8.1.3. Level III Threats. Level III threats have the capability of projecting combat power by air, land, or sea, anywhere into the operational area. Level III threats necessitate the command decision to commit a tactical combat force or other significant available forces in order to counter the threat. This threat level is beyond the capability of base defense and response forces.

4.8.2. Terrorist threat levels are a product of the following four factors:

4.8.2.1. Operational Capability. This factor focuses on the attack methods used by the group and other measures that enhance its effectiveness, such as state sponsorship and ingenious use of technology. The key element is whether the group has the capability and willingness to conduct large casualty producing attacks, for example a

suicide vehicle bomb containing thousand of kilograms of explosives or weapons of mass destruction timed to kill the most personnel at the target. Groups that selectively assassinate individuals or conduct late night bombings causing limited property damage pose a decreasing threat. The ability to operate on a regional or transnational basis and the overall professionalism of the group is also assessed.

4.8.2.2. Intentions. This factor is the stated desire or history of terrorist attacks against US interests. Recent substantial attacks in the country or, if the group is transnational, the conduct of operations in other countries is the higher end of the threat scale. This is especially true if the intentions are anti-DoD. The basis of the group ideology, whether the group is more focused on the host nation rather than US interests is the other key component. Whether the group will react to high profile US led international events, such as intervention in the Balkans, is also considered and rated.

4.8.2.3. Activity. This factor is an assessment of the actions the group is conducting and whether that activity is focused on serious preparations for an attack. The highest threat is credible indications of US targeting to include the movement of key operatives, final intelligence collection and movement of weapons to the target vicinity. Less threatening actions are contingency planning, training and logistical support. Activities that would make the group less likely to attack, such as robust fund raising or effective safe haven are considered. Whether the group has recently been disrupted by arrests or strikes on training camps will reduce the threat, at least in the short term.

4.8.2.4. Operating Environment. This factor rates how the overall environment influences the ability, opportunity and motivation to attack DoD interests in a given location. An important element of this factor is the capability of the host nation security apparatus to combat terrorism, its degree of cooperation with the US and the quality of the reporting on terrorist groups in the country. A key element is whether there is a DoD presence and if so the type, size, location, political sensitivity and if temporary, its duration. It is also important to consider if the group is focused on DoD as its primary target for anti-US attacks. Another part of this factor is the overall political, economic and military stability of the country and its effect on the ability of a group to attack.

4.8.3. Insider Threat. All Airmen need to understand and be prepared for the wide range of motivations and methods, including self-radicalization, distress over relationship problems, association with hate groups, and resentment over perceived personal and professional slights by others within the organization. Detecting and defeating these internal threats requires close personal observation and interaction with co-workers. For example, the threat could possibly come from an enemy agent who has infiltrated our ranks or from a disgruntled coworker with the intent to harm base personnel or damage Air Force resources. Our ability to assess this potential threat to military operations is difficult. Our best defense against this type of threat is increasing our awareness of its potential existence and to remain aware of possible indicators or warning signs which could include, but are not limited to, negative statements, adverse behaviors and noticeable changes in conduct.

4.9. Minimizing the Threat. What can you do to minimize these threats?

4.9.1. Maintain an awareness of the enemy's aims, objectives, and subversive techniques.

4.9.2. Develop a sense of personal dedication to national policy.

4.9.3. Report to and discuss with your supervisor any activity appearing to be subversive or suspicious.

4.9.4. Employ entry and internal control of personnel within your restricted area.

4.9.5. Guard against the possible use of force to gain entry into a restricted area.

4.9.6. Know the security procedures within your duty area. Contact your immediate supervisor when in doubt on any security policies.

4.9.7. Know your security reporting and alerting procedures.

4.9.7.1. When any threat indicators, suspicious activity, or hostile event occurs, immediately call the Base Defense Operation Center (BDOC), ext (895-3669) or by using a direct access line. If no phone is available but you have radio contact through your control center, have your control center contact BDOC. Another option is to flag down a security forces patrol. DON'T HESITATE.

4.9.8. Avoid complacency. Be aware that individuals intent on damaging Air Force resources will use an assortment of different methods to gain entry into a restricted area. For example, the use of impersonations may be attempted. A person looking, talking, and acting as either a bona fide officer, airman, telephone repair person, or a fire inspector may in reality be an enemy agent.

4.9.9. Establish control systems to ensure only those with a NEED TO HAVE ACCESS to our protection level resources or classified information are granted access. Employ physical safeguards like safes, fences, lights, and anti-intrusion alarms to hinder espionage activities.

4.9.10. Question anyone you either do not recognize or do not see wearing their RAB. Check all persons in your duty area for proper identification to include badge and proper area number designator. Just because someone has a RAB does not necessarily mean they are authorized into a particular restricted area.

4.9.11. Know the proper area number on the badge for entry into the restricted area. When checking someone's RAB, look it over carefully and make certain the number for the area is not blotted out. Know your base's locally devised codes for RABs. If you discover an individual has a badge, and either the proper area number is not open or some other portion of the badge is incorrect, contact security forces and have the individual checked out. Don't be quick to accept an individual's claims or excuses. Individuals either on temporary duty or transiting your base may be using their home-station RAB. When checking the RAB of an individual from another installation, ensure the individual is listed on a current Entry Authority List (EAL) authenticated by a supervisor from the local Security Forces Squadron.

4.9.12. Look for additional information concerning the use of RABs and EALs in AFI 31-101, Chapter 7. If some uncertainty exists in any situation, contact the SF before letting the individual proceed. Be alert and don't take anything for granted.

4.9.13. Remove and secure your RAB upon departing the restricted area to reduce the possibility of unauthorized use or counterfeiting.

4.10. Knowing the Threat. Our mission is weakened as long as our base is vulnerable to clandestine activities like terrorism, espionage, and sabotage. We can eliminate this weakness only by YOUR active participation in our security system. To accomplish this, you must be knowledgeable of the local threat (identify any unclassified local threat information).

4.11. The Integrated Defense Reporting and Alerting System.

4.11.1. Purpose. The Indicator and Incident Reporting system is an integral part of the Integrated Defense Program is the Security Reporting and Alerting System. This section acquaints you with the system and your responsibilities. Observant ID and support forces are the first line of defense against threats, but often fail to recognize or report behaviors of significant security concern. This indicates a need to educate personnel about a clearly defined set of indicators when an individual may be engaging in espionage or other egregious behavior that must be reported. The following reports will be utilized to report any suspicious or confirmed hostile activity:

4.11.2. Reports and Conditions. By using up-channel reports, down-channel reports, and Force Protection Conditions (FPCONs), we keep personnel at all levels informed of activities affecting the security of our protection level resources. Understanding when and how they are used is essential to the effectiveness of the Security Reporting and Alerting System.

4.11.3. Up-Channel Reports. The two types of up-channel reports used to alert command centers of possible and actual hostilities are Indicator Reporting (SALUTE) and COVERED WAGON reports.

4.11.3.1. Security Incidents Reporting. Any threat indicators or suspicious activity towards PL 1, 2, 3 resources should be reported to the BDOC immediately at 895-3669/3670, through the Security Incident Reporting Line at 895-2222 or from the Flightline Hotline. The recommended format is the "Size, Activity, Location, Uniform/Unit, Time, Equipment (SALUTE)" report as described in AFPAM 10-100, Airman's Manual. Supervisors at all levels must ensure all Airmen understand specifically what activities and behaviors are considered suspicious and reportable based on the local threat.

NOTE: "HELPING HANDS" are no longer required "code words" used during up-channeled notifications.

4.11.3.1.1. Security Incidents Reports are made to BDOC who may relay them to the installation command post. Security incidents reporting identifies suspicious activity affecting Protection Level 1, 2, or 3 resources at an installation or dispersed site. Most installation command posts don't relay this report to higher headquarters since it reflects a situation not fully investigated or analyzed.

4.11.3.1.2. Incidents must be investigated by on-duty security forces. A security team will determine if the event is hostile or non-hostile (i.e. procedural violation, authorized individual failed to wear a RAB, etc). In non-hostile cases the SALUTE report will be cancelled by on-duty security forces based on local instructions and guidance.

4.11.3.1.3. For SALUTE report situations determined to be hostile, on-scene security forces will immediately notify BDOC, who then up-channels the COVERED WAGON report to the installation command post. The installation command post up-channels the COVERED WAGON report to the HQ ACC Command Center.

4.11.4. COVERED WAGON Reports.

4.11.4.1. COVERED WAGON reports inform Higher Headquarters (HHQ) that an unusual incident affecting PL 1, 2, or 3 resources, probably or actually hostile, occurred at an installation or dispersed site. Reportable incidents will be up-channeled by the BDOC through the Installation Command Post in accordance with the appropriate Operational Report (OPREP) category (i.e., OPREP 3) and procedures specified in AFI 10-206, *Operational Reporting*. Regardless of severity, the installation command post will submit COVERED WAGON reports concerning any attack on, or deliberate invasion of, a restricted area by unauthorized personnel with the intent and capability to damage PL 1, PL 2, or PL 3 resources, or disrupt the mission. COVERED WAGON reports will also be submitted when actual intentional damage occurs to PL 1, PL 2, or PL 3 resources regardless of severity (i.e., hammering or splashing paint on an aircraft, etc).

4.11.4.2. Initiating COVERED WAGON Reports. Incidents are reported to the BDOC by any means available by anyone who witnesses or discovers an incident. The BDOC generally sends COVERED WAGON reports to the local Command Post. Transmit reports by the fastest means available consistent with security constraints. Air Force units will immediately submit an initial voice report to the appropriate command center via telephone. ***NOTE:*** Do not delay an initial report due to lack of information.

4.11.4.3. The Installation Command Post will relay COVERED WAGON reports directly to HQ ACC Command Center. Identify the affected resource's owning Major Command in the COVERED WAGON report. Additionally, if the affected resource belongs to a tenant unit or is a transient resource, this information must also be included in the report. The installation command post is responsible for assigning a covered wagon tracking number (e.g. 01-10; the first number is the number of covered wagons the installation has had and the second number is the year).

4.11.4.4. Canceling COVERED WAGON Reports. The Installation Commander or designee may cancel the COVERED WAGON incident. Cancellation actions are taken when the situation has been satisfactorily resolved and all required actions associated with the incident are complete. When security forces declare a COVERED WAGON, each unit implements increased security measures based upon the appropriate FPCON procedure in their IDP.

4.11.5. Down-Channel Alerting.

4.11.5.1. The Force Protection Condition Alerting Message (FPCAM) is a down-channel alerting order that sets in motion an increase in security readiness posture. When either the number of active up-channel reports, or intelligence indicators show actual or the potential for coordinated or widespread hostile activities, a FPCAM is used to alert installation commanders of the need to increase their security readiness.

4.11.5.2. The Air Force Operations Support Center or ACC Command Post transmits a FPCAM electronically to installations. As a general rule, the message does not implement a theater-wide or Air Force-wide FPCON. The message provides a synopsis of the situation leading to the release of the message and recommended courses of action. The FPCAM provides commanders the flexibility to tailor their FPCON implementation actions to their local situation. However, if the alerting message mandates the implementation of a certain FPCON, then implementation is mandatory and can only be canceled by the originator.

4.11.6. FPCON Alerting Message. FPCONs may be generated by a FPCAM or declared locally by the Installation Commander. Events that may trigger a FPCAM include intelligence indicating a potential or imminent attack, advance warning of civil disturbances or demonstration, or need for force generation.

4.11.6.1. FPCON reports are a rapid security communications system integrating all USAF bases and commands through a series of up-channel and down-channel reports. Local Command Posts report FPCON changes (via up-channel reporting) to HHQ. The FPCON alerting process for down-channel messages starts at higher-level headquarters and passes down through channels. Through this system either a hostile or possibly hostile event at one location, or a pattern of seemingly unrelated happenings at several locations, can serve as a basis for swift security alerting or warning throughout the USAF.

4.11.7. There are five FPCONs:

4.11.7.1. FPCON NORMAL: A general threat of possible terrorist activity exists, but warrants only a routine security posture.

4.11.7.2. FPCON ALPHA: This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO. The measures in this FPCON must be capable of being maintained indefinitely.

4.11.7.3. FPCON BRAVO: This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

4.11.7.4. FPCON CHARLIE: This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this FPCON for more than a

short period will start to create hardships and affect the peacetime activities of the unit and its personnel.

4.11.7.5. FPCON DELTA: This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely.

4.11.7.6. Security Measures: Refer to Shaw AFB 10-245 AT/FP Plan for the measures in each FPCON.

4.12. Control of Entry and Movement of Personnel Within Restricted Areas. An essential part of the security program is controlling personnel entry into restricted areas and their movement once inside. Entry into restricted areas, and movement of personnel within restricted areas, must be limited not only to those absolutely requiring entry to perform their official duties, but also to those who have been granted specific authority.

4.12.1. Entry Authority. The two types of entry authority to restricted areas are escorted and unescorted.

4.12.2. Unescorted Entry. Persons authorized by the commander responsible for the restricted or controlled area grants unescorted entry because of a regular and recurring need to enter the restricted or controlled area.

4.12.3. Escorted Entry. Personnel that do not have unescorted entry authority and have an official need to enter a restricted area, but not on a frequent basis, must be escorted into restricted or controlled areas. In these instances, an escort official for the restricted area must validate the visitor's need to enter the restricted area. The escort official is responsible for the visitor's actions while inside the area and ensures the safe and secure conduct of the visitor.

4.12.4. Escort Officials. All personnel issued a RAB will be trained as an escort official. No additional "approved escort official" markings are required, but at Shaw Air Force Base, an escort official authorized to escort personnel within a specific area is identified by an "E" typed next to the open restricted area number on the USAF RAB.

4.12.4.1. The escort official meets the visitor at the entry control point, verifies their identity and need to enter the restricted area, registers the visitor on an AF Form 1109, *Visitor Register*, if required, and gives a briefing on security procedures prior to entry.

4.12.4.2. The escort official may designate another person to escort the visitor while in the area. The designated person must have unescorted entry for the area and cannot delegate this escort duty to any other personnel. The original escort official is still responsible for the visitor while the visitor is in the restricted area.

4.12.4.2.1. At manned entry control points, visitor(s) may only hand carry those items essential to the visit. The escort official in the presence of the entry controller must search all hand-carried items and vehicles driven by the visitor.

4.12.4.2.2. At unmanned entry, personnel entering restricted areas are responsible for searching and clearing all items in their possession (i.e., vehicle and hand carried items).

4.12.5. Entry and Internal Circulation Controls.

4.12.5.1. Entry Control. The USAF RAB serves as an official document issued to personnel who have been granted unescorted entry authority. RABs are designed with a series of numbers, which are either open or blocked out, to indicate specific restricted areas a person is authorized to enter unescorted. There are two types of badge systems used to control entry to USAF restricted areas. The Automated Entry Control System Level III and exchange badge system is designed for nuclear restricted areas. It is a positive entry control method based upon the exchanging of one RAB for an identical badge maintained at the entry control point of the area to be visited. The single-badge system designed for nonnuclear areas is the most frequently used. Since the single-badge system can be defeated with relative ease, the entry controller uses at least one of the following supporting identification or verification techniques prior to allowing entry.

4.12.5.1.1. Personal Recognition. This is the most reliable means of verification if the number of personnel is relatively small. You personally recognize the people who routinely work within the restricted area. Personnel are also required to have a restricted area badge in their possession prior to entering the restricted area.

4.12.5.1.2. Signature and Credential Checks. A person can be asked to sign their name, recite their SSN, or show an ID card. The security force entry controller can use supplementary identification credentials other than the ID card.

4.12.5.1.3. EALs must identify whether or not an individual is authorized unescorted entry or requires an escort. In addition, EALs must contain the following information to enhance identity verification:

Name, OFF/ENL/CIV, and last six numbers of the SSN.
Organization.
Badge number.
Clearance status.
Dates of visit.
Expiration date of the EAL.

4.12.5.1.3.1. A SF supervisor, (E-6/GS-7 or above (or other civilian equivalent)) will be responsible for validating and authenticating the EAL. Authenticate the EAL by writing the following information near the bottom of the document: printed name/rank of authenticator, signed name of authenticator, date and time authenticated, page number authenticated (i.e., page 1 of 3, if there are multiple pages).

4.12.5.2. Telephone or Radio Verification. The procedure for using telephone or radio verification here at Shaw AFB is crossed checked with Master Restricted Area Badge List, using full name, last four SS# and date of birth.

4.12.5.3. Sign and Countersign. The procedure for using sign and countersign when Entry Control Points (ECPs) are posted here at Shaw AFB is set for emergency vehicles only (i.e. ambulance, fire, SF) and will change every six months along with the wing duress words. **Example:** If the number was five, then the posted sentry

would signed the driver with his or her hand with three finger and driver would respond with a two. Failure to comply will require the vehicle to stop and follow normal procedures.

4.12.5.4. Duress Codes. A duress code is a predetermined word passed during normal conversation indicating a duress situation. All personnel working within PL 1 and 2 restricted areas will know the duress code and how to use it. Unless required by the Installation Integrated Defense Council, personnel other than security forces working within PL 3 restricted areas are not normally required to know the code. The local Defense Force Commander establishes the duress code and all personnel must protect the code against inadvertent disclosure. If someone passes you the duress code, immediately contact security BDOC at (895-3669) and report a duress situation in progress. DO NOT alert others in the area of your intentions to contact security forces if this might endanger their lives.

4.12.5.5. Internal Circulation Control. The fundamental objective of an entry control procedure is to establish the identity of each person who seeks to enter. Security doesn't stop there. Movement within the area must also be monitored and is the purpose of internal controls. If a saboteur or terrorist is able to penetrate the outer perimeter undetected, the last line of defense is those working within the area … in other words--YOU. If you have made every effort to identify the person and an individual's identity can't be determined, contact the Security Forces BDOC, ext 2222, immediately and request assistance.

4.13. Individual Program Responsibilities.

4.13.1. The one basic requirement for everyone is IMMEDIATE RECOGNITION AND REACTION TO HOSTILE ACTS. Here are the actions necessary to effectively control and counter either hostile or possibly hostile events. What follows is a simplified effort to explain HOW YOU can meet your security obligation while performing duties in a restricted area.

4.13.2. First and foremost, you must be ALERT. Know who and what is going on around you at all times. Be alert for unauthorized personnel in the area. As you approach individuals, look for their RABs. If they have proper badges, and you recognize them, resume your duties. If they have badges, but are not recognized, check the RABs further. Determine if they have not only the authority but also an official reason for being in the area.

4.13.3. DETECT hostile acts possibly affecting our protection level resources. Look for abnormal equipment conditions to include cut wires, improper positioning, and visual signs of tampering. Be alert for damage to protection level resources to include bullet holes, gouges from objects used to strike the resource, or other types of damage.

4.13.4. Upon detection, ALERT OTHERS in the immediate area. Yell loud and clear for help/assistance. If you hear the alarm, safety permitting, stop what you are doing and assist. Either noise levels or extreme distances may prevent personnel from hearing the alert. In these situations visual signals are necessary.

4.13.5. After alerting others in the area when an unidentified person is found, you have the twofold responsibility of reporting the incident to BDOC by phone or radio through

your control center and detaining the individual. Accomplish these tasks simultaneously to the best of your ability.

4.13.6. Your responsibilities become relatively simple if other personnel are immediately available. You obtain their assistance to detain and move the unidentified person away from the protection level resources in the area. You then run to the nearest telephone or vehicle radio and report the nature and location of the incident to BDOC. If a SF patrol is in the area and readily available, attract their attention. What if no other personnel are available to assist?

4.13.6.1. The obligation of detaining an unauthorized person, and promptly reporting the incident, may require you to accomplish one task at the expense of another. In such instances, you must accurately evaluate the number of suspects, and in the case of a lone individual, the suspect's comparative physical stature. You must quickly determine if they possess weapons and the extent of damage they could possibly inflict on our critical resources. These considerations must be compared with the time it would take you to report the incident to BDOC and receive assistance from the SF. Accomplish both tasks simultaneously if possible.

4.13.6.2. If the situation is obviously beyond your capability to control, report the incident to BDOC as rapidly as possible. Stay cool and speak plainly when reporting. Don't omit the WHAT and WHERE of your report. SF requires these two factors in order to dispatch the help you need.

4.13.6.2.1. After you make the report, return to the area where the suspect was last seen. Attempt to relocate the suspect and keep this individual under observation. Look for the SF patrol and attract their attention so they will arrive on scene at the earliest possible moment. Meet the SF patrol and report the incident along with any other pertinent information you have. Explain what happened. The information you give the SF is the basis for their necessary counteractions. SF may call upon you to assist in searching the area, as required.

4.13.7. It is no exaggeration when we say our combat capability is placed in unnecessary jeopardy if we fail to carry out our individual ID responsibilities. It is everyone's responsibility to DETECT and REPORT hostile or possibly hostile events, and DETAIN unauthorized persons when possible.

4.14. Key Installation Defense Documents.

4.14.1. Installation Defense Plan (IDP). The IDP is the basic planning document for installation defense planning. Contingency plans are those plans dealing with events that could possibly occur at an installation.

4.14.2. Local Threat Assessment. Threat is assessed in a series of steps that result in threat ratings for unwanted events. Unwanted events are expressed as target-tactic pairs, and can best be understood as the loss or damage to an (asset/target) due to a (tactic). The local threat assessment identifies adversary types in the local area and calculates the Adversary Threat Level. Based on the Defense Threat Assessment (developed by the Air Force Office of Special Investigations) and the local threat analysis, a list of adversaries known or thought to be in the local area is produced, and an "Adversary Threat Level" is calculated for each.

5. Phase II (Annual) Physical Security Awareness Training.

5.1. Objective. This phase is ongoing and is designed to keep everyone apprised of threats, security procedures, and mission changes affecting them. This phase is completed annually and must be documented by unit training officials using any approved record system.

5.2. The requirement for phase II annual training can be met through commander's call briefings, formal classroom lecture, read and sign instructions, etc.

5.2.1. In addition to annual briefings, a method of determining the effectiveness of the installation program through detection exercises in restricted and controlled areas must be conducted. This requirement is satisfied by a viable Flightline Protection Program (FPP).

5.3. Flightline Protection Program. The FPP focuses specifically on evaluating the effectiveness of physical security awareness training while continuously improving the level of security awareness of personnel. The 20 FW/CC designates a wing FPP manager to promote a program of joint responsibility with owner/user personnel by assuring the highest level of security awareness.

5.4. FPP Exercises. The FPP manager coordinates exercises with unit FPP monitors and/or security managers in Shaw AFB PL 3 restricted areas. The ACC goal and minimum acceptable level for detection of an unauthorized individual inside a PL 3 area is less than 15 minutes, 70 percent of the time.

5.4.1. Personnel selected as perpetrators will have unescorted entry authority for the selected exercise location. Perpetrators may use altered or fake RABs. Perpetrators may attempt to enter the restricted area overtly (such as crossing a restricted area boundary at a place other than the ECP) or covertly (i.e., no RAB displayed). The perpetrator will have a real RAB available and displayed upon termination of the exercise. If owner/user personnel challenge a perpetrator and the challenge is properly upchanneled, the exercise is considered a detection. If the perpetrator has contacted three or more owner/user personnel or has not been detected or challenged within 15 minutes, the exercise is terminated and reported as a nondetection. Successful detections include proper challenging and identification procedures, as well as proper security reporting and alerting procedures. Perpetrators will not use simulated weapons or explosive devices and will not attempt to flee anyone requesting identification.

5.4.2. Personnel may also be verbally quizzed on proper challenging and notification procedures (i.e., location of Covered Wagon phones, Covered Wagon numbers, etc).

5.4.3. Quarterly reports are submitted to HQ ACC/SFOS identifying the quarterly detection rate, exercise type (over/covert), and result (detect/nondetect).

6. Training Escort Officials.

6.1. All personnel designated as escort officials for Protection Level 2 resources must be formally trained and certified on the duties and responsibilities of an escort official. Affected units conduct this training as part of Phase I and II training and must administratively track and document the training and certification process.

6.1.1. Escort official procedures are incorporated into the test located at Attachment 3 and must be administered to escort officials. Escort officials must recertify annually or when any significant change occurs in escort procedures.

6.2. Conclusion. A lack of emphasis on security awareness training will ultimately create a complacent attitude among the personnel working near our protection level resources. Commanders and supervisors have the responsibility of ensuring personnel are working together as a team against threats to our protection level resources. Individuals and groups who make plans to carry out threats against the United States Air Force are only as successful as we allow them to be. Your active participation in the Integrated Defense Awareness Training Program is a vital part of making our resources as unattractive a target as possible.

CLAY W. HALL, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPAM 10-100, *Airman's Manual*, 1 March 2009

AFI 10-245, *Antiterrorism (AT)*, 30 March 2009

AFI 31-101_ACCSUP, *Integrated Defense*, 15 February 2011

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 31-1, *Integrated Defense*, 28 October 2011

SAFB Plan 31-101, *Integrated Base Defense Plan*, 1 August 2011

Adopted Forms

AF 847, *Recommendation for Change of Publication*

AF 1199, *USAF Restricted Area Badge*

AF 1109, *Visitor Register*

Abbreviations and Acronyms

ACC—Air Combat Command

AF—Air Force

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information System

AT—Antiterrorism

BB—Base Boundry

BDOC—Base Defense Operation Center

BSZ—Base Security Zone

CONUS—Continental United States

DoD—Department of Defense

EAL—Entry Authority List

ECP—Entry Control Point

FPCAM—Force Protection Condition Alerting Message

FPCON—Force Protection Conditions

FPP—Flightline Protection Program

HHQ—Higher Headquarters

HQ—Headquarters

ID—Integrated Defense

IDP—Installation Defense Plan

JP—Joint Publication

OCONUS—Outside Continental United States

OPR—Office of Primary Responsibility

OPREP—Operational Report

PL—Protection Level

RAB—Restricted Area Badge

RDS—Records Disposition Schedule

SAFBI—Shaw Air Force Base Instruction

SATCOM—Satellite Communications

SF—Security Forces

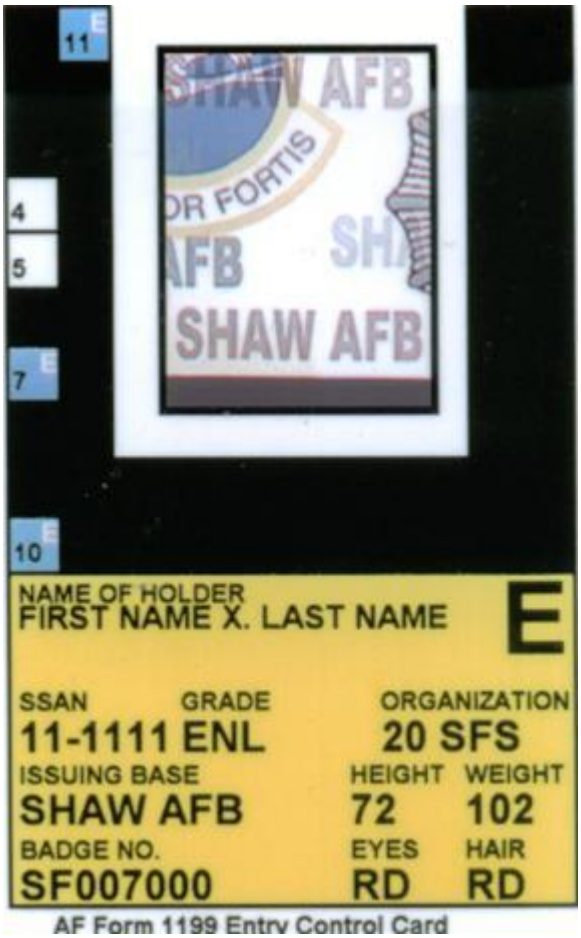
USAF—Unites States Air Force

Attachment 2

SAMPLE USAF RESTRICTED AREA BADGE AF FORM 1199

NOTE: The identifying techniques for Shaw AFB are the picture with the **MULTI-COLORED** background and the **SW0000** badge number series.

Figure A2.1. SAMPLE USAF RESTRICTED AREA BADGE AF FORM 1199



Shaw AFB Areas. The following are designated areas on the Shaw RAB:

Area #4 – F-16 Mass Parking Areas; Protection Level 3.

Area #7 – Wing Command Post; Protection Level 3.

Area #10 – Non-nuclear Munitions Storage Area; Protection Level 4/Controlled Area.

Area #11 – 20 OSS Vault; Protection Level 4/Controlled Area.

Attachment 3

INTEGRATED DEFENSE AWARENESS TRAINING EXAM

1. The objective of Integrated Defense (ID) Awareness Training is to:
    a. instill in every Airman a sense of responsibility for securing Protection Level (PL) resources
    b. instill in every Airman a sense of responsibility for securing all Air Force resources
    c. meet the minimum requirements of AFI 31-101, Integrated Defense
    d. train all base personnel in security forces tactics and procedures in order to protect PL resources

2. The goal of ID is to:
    a. neutralize safety incidents throughout the base boundary in order to ensure safe AF operations
    b. neutralize security threats throughout the base boundary in order to ensure unhindered AF operations
    c. meet the requirements of AFI 31-101, Integrated Defense
    d. train all base personnel in security forces tactics and procedures in order to protect PL resources

3. Protection Level designations reflect all of the following *except*?
    a. The importance of the resource to the overall US warfighting capability
    b. The known or postulated threat to the resource
    c. The alert status of the resource
    d. The political insignificance of the resource to the US

4. Which PL designation is associated with weapons systems capable of being on alert status?
    a. PL 1
    b. PL 2
    c. PL 3
    d. PL 4

5. Which PL designation is associated with Arms, Ammunition, and Explosives; POL/LOX storage areas; and aircraft parts warehouses?
    a. PL 1
    b. PL 2
    c. PL 3
    d. PL 4

6. Which PL designation is associated with nonnuclear alert forces or expensive, one of a kind systems?
    a. PL 1
    b. PL 2
    c. PL 3
    d. PL 4

7. Shaw AFB currently has two restricted areas containing PL 2 resources.
    a. True
    b. False

8. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion.
    a. True
    b. False

9. Small-scale, irregular forces conducting unconventional warfare that can pose serious threats to military forces and civilians would be classified as:
    a. Level I
    b. Level II
    c. Level III
    d. None of the above

10. Organizations that have the capability of projecting combat power by air, land, or sea, anywhere into the operational area are likely:
    a. Level I
    b. Level II
    c. Level III
    d. None of the above

11. If you detect a security incident or hostile act, you should call:
    a. Base Defense Operations Center at 895-3669/3670
    b. Security Incident Reporting Line at 895-2222
    c. Flightline Hotline
    d. Any of the above

12. While working in a restricted area, you notice an individual you don't recognize, who is wearing a restricted area badge, but is acting suspiciously. What should you do?
    a. Nothing, as long as they are wearing a restricted area badge with the proper area open
    b. Nothing, as long as they are wearing a restricted area badge
    c. Check them out and determine if they are authorized to be in the area
    d. Notify security forces immediately

13. While standing in line at an off-base convenience store, you notice a major whose restricted area badge is exposed. What is the appropriate course of action?
    a. Do nothing; it is common for people to forget to remove their badge after departing the restricted area
    b. Do nothing; it is not your responsibility to inform personnel of the need to remove their badge when not in a restricted area
    c. Inform the major his restricted area badge is displayed and ask him to hide it from public view
    d. Get the major's name and contact security forces so an incident report can be filed

14. An Indicator Report is more serious than a Covered Wagon.
    a. True
    b. False

15. What are the two types of entry authority into a restricted area?
    a. Escorted
    b. Unescorted
    c. Exempted
    d. Emergency
    e. Both a & b

16. What are the four factors involved in categorizing terrorist threat levels?
    a. Operational Capability
    b. Intentions
    c. Activity
    d. Operating Environment
    e. All of the above

17. Detecting and defeating internal threats requires:
    a. close personal observation
    b. interaction with co-workers
    c. both a & b
    d. neither a nor b

18. All of the following statements concerning minimizing the threat are true, *except*:
    a. Maintain an awareness of the enemy's aims, objectives, and subversive techniques
    b. Employ entry and internal control of personnel within your restricted area
    c. Guard against the possible use of force to gain entry into a restricted area
    d. Establish loose controls to facilitate ease of entry into restricted areas

19. When escorting an individual into a restricted area, you are responsible for what?
    a. Verifying the identity and need of the individual to enter the restricted area
    b. Registering the individual on the AF Form 1109, Visitor Register Log
    c. Giving a briefing on security procedures prior to entry
    d. All of the above

20. An escort official may delegate escort duties to another person, with the appropriate area open on their restricted area badge, once visitors have been escorted into the restricted area.
    a. True
    b. False

21. Once an escort official delegates escort duties to another person, that person may delegate escort duties to anyone with the appropriate area open on their restricted area badge.
    a. True
    b. False

22. Which Force Protection Condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent?
    a. Normal
    b. Alpha
    c. Bravo
    d. Charlie
    e. Delta

23. A report made to BDOC of suspicious activity involving PL 1, 2, or 3 resources is called _____.
    a. Indicator Reporting
    b. Covered Wagon Reporting
    c. Force Protection Condition Alerting Message Reporting
    d. Broken Arrow Reporting

24. A report informing higher headquarters that an unusual incident affecting PL 1, 2, or 3 resources, probably or actually hostile, occurred at an installation or dispersed site is called a(n)_____.
    a. Indicator Report
    b. Covered Wagon
    c. Force Protection Condition Alerting Message
    d. Broken Arrow

25. Which of the following is a down-channel report?
    a. Indicator Report
    b. Covered Wagon
    c. Force Protection Condition Alerting Message
    d. Broken Arrow