

**BY ORDER OF THE COMMANDER
FAIRCHILD AIR FORCE BASE (AMC)**

**FAIRCHILD AIR FORCE BASE
MANUAL**



31-104

17 JUNE 2021

Security

**PRIMARY SECURITY COORDINATOR
PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: Access to this publication is restricted; this publication may be released to Department of Defense (DoD) personnel only; requests for accessibility outside of the DoD must be approved by the OPR

OPR: 92 SFS/S5

Certified by: 92 ARW/DFC
(Maj. Brian S. Slater)

Supersedes: FAFBMAN 31-104,
26 Nov 18

Pages: 32

FAIRCHILD AFBMAN 31-104 is directive in nature and failure to adhere to the standards set out in this manual may form the basis for adverse action under the Uniform Code of Military Justice (UCMJ) and AFI 36-704, *Discipline and Adverse Actions*. An example would be a dereliction of duty offense under Article 92. As used in this manual, “Shall” or “Will” or an action verb in the imperative sense means a procedure is mandatory. “Should” means a recommended procedure. “May” means an optional procedure. To the extent its directions are inconsistent with other FAFB manuals, the information herein prevails. Units tasked by this manual must initiate procedures to support any procedural changes. There are prohibited practices and specific requirements throughout this manual. Violations of the specific prohibitions and requirements of this manual by military personnel may result in prosecution under the UCMJ. Violations of this manual by Air Force civilian employees may result in appropriate disciplinary action without regard to criminal liability. Administrative action, such as a reprimand, may be taken with regard to military members and civilian employees who violate any requirements of this manual even if such violations do not constitute criminal misconduct. This manual applies to all personnel assigned to Fairchild Air Force Base (AFB), both military and civilian, guard and reserve, as well as transient or personnel.

The FAFB Primary Security Coordinator Manual is being published by the Defense Force Commander in accordance with the requirements of 92 ARW Plan 31-1 (Integrated Defense). This

manual promulgates requirements contained in AFI 31-101, *Integrated Defense*. To the extent there is a disagreement between this manual and any HHQs directives, the HHQs directives will prevail.

This manual provides information and "how-to-guidance" for establishing and maintaining an effective Resource Protection/Crime Prevention Program on Fairchild AFB. In addition, it provides helpful information on "best business practices" and "lessons learned." This manual applies to active duty AF military; Air National Guard (ANG); AF Reserve Command (AFRC); AF civilian employees; and all Department of Defense (DoD) contractors as prescribed in AFI 16-1406, *Industrial Security Program*, when contract performance depends on access to AF information.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records disposition Schedule (RDS), or any updated statement provided by the AF Records Management office (SAF/CIO A6P). This manual requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by 5 USC 552a. Systems of records notice F024 AF IL C applies. Ensure all records created by this manual containing For Official Use Only (FOUO) information, including privacy records, are marked IAW Department of Defense (DoDM) 5200.01-V1, *Information Security Program*, and AFI 33-332, *Air Force Privacy and Civil Liberties Program*. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

Chapter 1 - CRIME PREVENTION PROGRAM MANAGER (CPPM) was revised. IAW AFI 31-118, *SF Standards and Procedures*, the crime prevention program is a function of Police Services. The DFC appoints in writing an individual to manage crime prevention functions. The DFC focuses resources based upon installation requirements. Police Services will provide semi-annual crime statistics, rates, and trend analysis to members of the Integrated Defense Working Group (IDWG) and Integrated Defense Council (IDC) and Traffic Statistics to the Traffic Safety Coordination Group (TSCG). Crime statistics will be pulled from two sources: Spokane County Sheriff's office provides monthly crime maps for larger area/off base crime statistics and AFJIS for FAFB crime rates. Traffic Statistics will be pulled from AFJIS.

Chapter 2 - UNIT RESPONSIBILITIES FOR CRIME PREVENTION was revised. Security is a function of command. The CPPM highly encourages unit commanders to establish crime prevention programs within their unit and suggest they designate a focal point to coordinate program activities within their unit. Primary Security Coordinators are simply a focal point for the CPPM to promote military and civilian community involvement and combat mutual crime problems. Primary Security Coordinators are identified by the Unit Commander and are recommended to be the Unit Security Assistants, Unit-appointed Training Personnel, or Unit Facility Managers. Ensure all sensitive high-theft items are properly marked and a descriptive

listing is maintained. The Custodian Authorization Custody Receipt Listing (CA-CRL) is recommended and is usually kept by the unit's equipment custodian.

Chapter 4 - INTEGRATED DEFENSE (ID) AWARENESS TRAINING (IDAT) was revised. The 92 ARW/CC renamed the IDAT program to "Security Education Training (SET)." Phase I training will still be conducted at Right Start by SF. Phase II training will remain with individual units and be overseen by the unit Security Assistant. SF Physical Security Section will still be available for guidance and assistance. Security Forces Pass & ID will ensure that all training is documented on the AF Form 2586 prior to issuing Restricted Area badges

Chapter 5 – OBTAINING A RESTRICTED AREA BADGE was revised. The 92 ARW/CC renamed the IDAT program to "Security Education Training (SET)." All references to the IDAT program have been replaced with SET. All references to Security Manager have been amended to state Security Assistant. Requirements for Phase II and escort training scores have been removed. Current DD Form 577 date was updated to reflect NOV 2014. DD Form 577 and AF Form 2586 examples have been replaced with current forms. **Paragraph 5.2.4** regarding AF Form 1199CD Letter for Bearer has been removed.

1.	CRIME PREVENTION PROGRAM MANAGER (CPPM).....	4
2.	UNIT RESPONSIBILITIES FOR CRIME PREVENTION.	5
3.	CRIME PREVENTION PROGRAMS.....	7
4.	SECURITY EDUCATION TRAINING (SET).....	8
Figure 4.1.	Controlled/Restricted Areas Escort Briefing	11
5.	OBTAINING A RESTRICTED AREA BADGE.....	12
Figure 5.1.	Duty Title.....	13
Figure 5.2.	Sample DD Form 577.	16
Figure 5.3.	Instructions for completing DD Form 577.....	17
Figure 5.4.	Sample AF Form 2586.....	18
Figure 5.5.	Reverse Side of Sample AF Form 2586.	19
Figure 5.6.	Page 3 of Sample AF Form 2586.....	20
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		23
Attachment 2—PRIMARY SECURITY COORDINATOR LETTER		25
Attachment 3—SET SELF INSPECTION CHECKLIST		26
Attachment 4—SAMPLE SET TRAINING EVALUATION CHECKLIST		28
Attachment 5—SECURITY EDUCATION TRAINING (SET) EXERCISE SAFETY BRIEFING		30
Attachment 6—USER FEEDBACK		31

1. CRIME PREVENTION PROGRAM MANAGER (CPPM).

1.1. **Commander's Intent.** IAW AFI 31-118, *SF Standards and Procedures*, The crime prevention program is a function of Police Services. The DFC appoints in writing an individual to manage crime prevention functions. The DFC focuses resources based upon installation requirements. The 92 ARW Crime Prevention Program (CPP) will provide a complete and in-depth program for the protection of government resources, equipment, funds, weapons, controlled substances, and facilities. Education of base personnel on crime prevention is vital to ensuring the protection of USAF resources. Installation commanders are responsible for developing and maintaining a Crime Prevention Program. The staff officer for the program is the Defense Force Commander (DFC).

1.2. **CPPM Objectives.** The CPPM has four primary objectives.

1.2.1. Maintain the Air Force war-fighting capability by reducing damage to Air Force personnel and resources.

1.2.2. Safeguard Air Force personnel and property by reducing the opportunity for criminal activity, theft, or terrorist attack by making a potential target inaccessible or unattractive.

1.2.3. Promote the use of the Crime Prevention through Environmental Design (CPTED) principles of natural surveillance, natural access control and territorial reinforcement.

1.2.4. Ensure that everyone safeguards personnel and government property on and off the installation.

1.3. **CPPM Responsibilities .**

1.3.1. CPPM Program Reviews. Conducts quarterly reviews of criminal statistical data to examine crime patterns, recommend crime prevention strategies and provide analyzed crime data to unit commanders, police services activities and other interested agencies.

1.3.2. Crime and Traffic Statistics. Police Services will provide semi-annual crime statistics, rates, and trend analysis to members of the Integrated Defense Working Group (IDWG) and Integrated Defense Council (IDC) and Traffic Statistics to the Traffic Safety Coordination Group (TSCG). Crime statistics will be pulled from two sources: Spokane County Sheriff's office provides monthly crime maps for larger area/off base crime statistics and AFJIS for FAFB crime rates. Traffic Statistics will be pulled from AFJIS.

1.3.3. External Police Services Agencies. CPPM maintains liaison with military/civilian organizations and authorities to provide the most comprehensive and up-to-date information for dissemination and cross-tell.

1.3.4. Community Relations. CPPM builds and maintains relationships with helping agencies in order to facilitate crime prevention message delivery and build connections with the community.

1.3.5. Helping Agencies. Police Services should make contact with agencies such as ADAPT, Drug Demand Reduction, Family Advocacy, and the Sheriff's Community Oriented Policing Effort (SCOPE) that have crime prevention programs and help develop plans and programs that target specific issues therein. These particular agencies work

largely with the community in addressing issues that are seen by Security Forces regularly so participation with them is highly encouraged.

2. UNIT RESPONSIBILITIES FOR CRIME PREVENTION.

2.1. **Unit Commanders.** Security is a function of command. The CPPM highly encourages unit commanders to establish crime prevention programs within their unit and suggest they designate a focal point to coordinate program activities within their unit. Primary Security Coordinators are simply a focal point for the CPPM to promote military and civilian community involvement and combat mutual crime problems. Primary Security Coordinators are identified by the Unit Commander and are recommended to be the Unit Security Assistants, Unit-appointed Training Personnel, or Unit Facility Managers. Unit commanders should develop, support, and maintain their unit program by accomplishing the following:

2.1.1. Provide 92 SFS/S5L with a letter (See Attachment #2) identifying primary and alternate Primary Security Coordinators for their personnel and high theft/value items. The level of unit security must reduce the opportunity for theft of or damage to resources. Owners/users of resources must be actively involved in security of their assets. Response is provided by Security Forces. Integrated Defense (ID) measures must, as a minimum, Anticipate, Deter, Detect and Assess threats or hostile acts to these resources.

2.1.2. Report all security incidents/violations (i.e., larceny, vandalism, penetration attempts, etc.) to the Base Defense Operations Center (BDOC) immediately.

2.1.3. Conduct self-inspections as required by applicable directives, instructions and plans.

2.1.4. Support the CPPM through active participation in CPP planning and programming phases to implement local procedures.

2.1.5. Ensure compliance with directives on access to restricted/controlled areas and PL 1-4 resources.

2.1.6. Assist in the development and implementation of the Integrated Defense Plan through involvement in designated working groups and active participation in the Integrated Defense Risk Management Process.

2.1.7. Identify all unit assigned high value assets and mission essential functions.

2.1.8. Comply with Security Forces directives, programs, procedures and local instructions.

2.1.9. Participate in emergency security and integrated defense operations as specified in integrated defense and emergency management plans.

2.1.10. Ensure that appropriate updated Operating Instructions, MOAs, MOUs are in place to facilitate participation in base security and emergency management instructions and plans. **Note:** The Unit Primary Security Coordinator is your key to providing a robust Unit Crime Prevention Program and meeting the 92 ARW/CC commander's intent.

2.2. Unit Primary Security Coordinators.

2.2.1. Be responsible to their commander for the proper management of unit personnel and areas not containing PL 1-4 assets. This responsibility includes knowing and implementing proper security control (physical and procedural) for the area.

2.2.2. Monitor all aspects of the area. In this respect, a formal review (self-inspection) of the area(s) must be conducted and documented semi-annually. If significant problems are discovered, the unit commander or staff agency chief must be briefed.

2.2.3. Assess the effectiveness of the CPP and identify Crime Prevention (CP) deficiencies in the unit/agency CP program. Do this by conducting formal, self-initiated exercises, building checks and personnel checks. Utilize information provided by the CPPM.

2.2.4. Your unit commander or general manager should identify you and an alternate as their unit Primary Security Coordinator in writing. Forward a copy of these letters to 92 SFS/S5L.

2.2.5. Ensure all personnel who work in or have access to the unit are aware of their responsibilities for resource protection/crime prevention.

2.3. Facility Custodians/Individual Responsibilities.

2.3.1. Ensure all work areas/offices are secured when not occupied.

2.3.2. Ensure exterior doors to work areas/buildings have locks (combination, cipher, etc.) installed or are secured with padlocks and hasps.

2.3.3. Ensure hinge pins located on outside of doors, gates, or containers used to protect sensitive, high-theft property are peened, pinned, or spot-welded.

2.3.4. Ensure general construction of building is kept in good condition so as to prevent unauthorized entry.

2.3.5. Ensure interior containers, lockers or cabinets are used to secure property when possible.

2.3.6. Ensure lockers or cabinets used for storage of sensitive high-theft items are locked any time they are not directly under the control of authorized personnel.

2.3.7. Ensure all sensitive high-theft items are properly marked and a descriptive listing is maintained. The Custodian Authorization Custody Receipt Listing (CA-CRL) is recommended and is usually kept by the unit's equipment custodian.

2.3.8. Ensure large equipment such as lawn and snow equipment are properly secured in designated storage areas when not in use. If storage area is not available, items will be secured to a structure with material strong enough to prevent theft, i.e., chain or cable and padlock.

2.3.9. Protect and mark government tools to meet the following minimal standards:

2.3.9.1. Secure all tools not in use. Provide toolbox racks with locking devices if the unit issues tools and toolboxes to personnel. Racks should be located in areas where activity or observation is present.

2.3.9.2. Engrave or mark tools and electronic equipment indicating owner unit to discourage theft. Tools that have serial numbers will be logged and kept at responsible section; if engraving electronic equipment would affect operation of, or deface it, it needs not be marked but be sure to log any and all serial numbers.

- 2.3.10. Ensure all vehicles not being used have ignition switches turned off. If parked outside, responsible individual will remove and maintain keys.
- 2.3.11. Lock all government vehicles when they are unattended with government property inside, i.e., radios.
- 2.3.12. Conduct a visual check of all work areas/offices, at beginning of each workday, being especially watchful for any indication of theft or illegal entry, actual or attempted. If any indications exist, ensure immediate area and any signs of evidence are protected until the arrival of Security Forces personnel.
- 2.3.13. Challenge anyone who is unknown or does not belong in the work center. If individual being challenged cannot produce positive identification or reason for being there, notify Security Forces immediately at 911.
- 2.3.14. Ensure everyone is familiar with emergency procedures, i.e., bomb threat, power outages, fire response, etc.
- 2.3.15. While conducting nightly closing procedures, turn on security lighting and always check to make sure they are operational.
- 2.3.16. Restrict personnel entrances and exits to as few as possible. This improves internal circulation control.
- 2.3.17. Ensure during any emergency that the best possible effort is made to secure and protect assigned resources.
- 2.3.18. At the end of each workday, properly secure all property, ensure all security containers, rooms/areas, windows, doors, gates, grills, etc., are locked, and all physical security aids are functioning as intended.

3. CRIME PREVENTION PROGRAMS

3.1. **Operation Crime Stop** : This program allows for witnesses to remain anonymous while reporting suspected or actual crimes. Police Services will ensure current dedicated Crime Stop line (509) 247-5555 is published to the public and monitored 24/7. All crime stop calls will be logged on the AF Form 53, Security Forces Desk Blotter. Operation Crime Stop helps overcome reluctance to become involved with Security Forces by providing a single telephone line for crime reporting while allowing witnesses to remain anonymous. Operation Crime Stop provides a safe way to report suspected or actual crimes anonymously. Anonymous crime reports can include school crimes, such as persistent bullying, domestic violence, suspicious activity, threatening acts or behavior, possession of weapons and or the use or sale of illegal drugs.

3.2. **Operation Identification (OPID)**: This program is a crime resistance technique which individuals use to deter burglaries and larcenies. It also provides investigative leads that increase the chances of solving crimes. Owners are encouraged to permanently mark their property with an identifying number. The owner should use the service prefix "AF-" followed by the owner's last name, plus last 4 digits of his/her social security number. If items that are not easily marked, or if owners do not wish to mark, they will be photographed. Encourage both marking and photographing.

3.2.1. CPPM will maintain one or more electric engravers. CPPM will also maintain a log to provide the base populace the ability to check out engravers for home use/return.

3.2.2. Engraving log should include personnel's name, cell/duty phone, squadron/office symbol, date/time out and date/time returned. Also use AF Form 1297 (Temporary Issue Receipt) when checking out engravers and maintain a copy in the binder with the log. Engravers will be checked out for a maximum of 48 hours.

3.2.3. Unit Primary Security Coordinators will also maintain engravers and log system within their own units to ensure government property is properly marked to mitigate theft and misuse.

3.3. Crime Hazard Identification Program: One goal of crime prevention is to identify, report and eliminate as many crime hazards as possible, thus reducing the opportunity for crime. Security Forces and base-level CPPM's may solicit and issue Crime Hazard Reports to commanders and agency chiefs for corrective actions. Security Forces should leave a Crime Hazard Reminder when they discover unsecure vehicles, office areas, equipment or unattended property. CPPM will aid unit Primary Security Coordinators in issuing Crime Hazard Reports to commanders and agency chiefs for corrective actions.

3.4. Citizen Awareness Program (CAP): This program is used to educate the base community on crime prevention. CPPM and unit Primary Security Coordinators will use all available resources to disseminate information on typical crimes, victims, and offenders. This is done in an effort to reduce/eliminate victimization of personnel and mitigate loss or destruction of private/government property.

4. SECURITY EDUCATION TRAINING (SET)

4.1. Executive Agent. The 92 SFS Commander (aka: Defense Force Commander) will implement the SET as the executive agent for ensuring integrated defense training is provided.

4.1.1. 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.

4.2. **Appointments.** The Defense Force Commander (DFC) must appoint a NCOIC of Physical Security in writing and inform all commanders of the appointment. The Installation Security Section (ISS) will publicize information affecting the SET program to unit Security Assistants or unit appointed training personnel for dissemination to all squadron personnel. The ISS representative may brief the IDC on the overall assessment of security awareness for the installation. The ISS Physical Security NCO will be available upon request to assist unit Security Assistants to guide SET programs compliance with this manual.

4.3. Unit Commander Responsibility:

4.3.1. Unit Commanders have overall responsibility for their organizations SET status.

4.3.2. Unit Commanders will ensure Security Assistants or unit appointed training personnel are in charge of their SET Program. These personnel should be familiar with and have a close working relationship with the ISS Physical Security NCO.

4.4. Unit Security Assistants/Unit-appointed Training Personnel Responsibility:

4.4.1. A self-inspection will be conducted IAW Wing Inspection Team (WIT) guidance by all units assigned to the 92 ARW and tenant units attached to Fairchild AFB. Unit Security Assistants or unit appointed training personnel may request a staff assistance visit (SAV) from the ISS Physical Security NCO. Unit Security Assistants or unit-appointed training personnel may utilize the recommended Self-Inspection Checklist provided at [Attachment 3](#).

4.4.2. Unit Security Assistants and unit-appointed training personnel are responsible for ensuring unit personnel attend Phase I (orientation) and Phase II (continuation) training. Unit Security Assistants and unit-appointed training personnel will document when SET training is completed. If unit testing is required, Security Assistants and unit-appointed training personnel will create a trend analysis on high missed test questions to assess the unit's overall SET program.

4.4.3. All training records will be maintained by unit Security Assistants and unit-appointed training personnel.

4.5. **Individual SET Responsibilities.** The one basic requirement for everyone is immediate recognition and reaction to hostile acts. In simpler terms, if you see something then say something.

4.6. SET Training Requirements:

4.6.1. SET 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.

4.6.2. The following is a brief summary of Phase I and Phase II training:

4.6.2.1. Phase I, Orientation Training. The ISS conducts this training during indoctrination to the installation. **NOTE:** Fairchild AFB accomplishes this requirement via the newcomer's right start briefing. Unit Security Assistants and unit-appointed training personnel are responsible for ensuring personnel not required to attend Right Start briefings receive this training. Orientation training is directed toward security procedures and requirements peculiar to the MAJCOM of assignment, the base, and the job of each individual. As a minimum, everyone must have a general knowledge of the threat, the installation's security instructions and plans, and the security reporting and alerting system to include methods of notifying BDOC of emergency situations. Unit Security Assistants or unit-appointed training personnel will ensure proper documentation and records reflect date of completion and will be maintained for 12 months in each squadron's individual records. Unit Security Assistants or unit-appointed training personnel will annotate all training dates in block III "DUTY" of the AF Form 2586. Units may require personnel to pass a standard security awareness test administered as part of Phase I training before granting unescorted entry to a restricted area.

4.6.2.2. Phase II Continuation Training. The unit, as part of their ancillary training program, conducts Phase II. Training should be tailored to the specific duties of their work centers and must be designed to keep everyone informed of threats, security

procedures, and mission changes that affect them. Phase II training should consist of an annual presentation that will be given to all unit personnel. Formal lectures, seminars, staff meetings, guardmount, conferences, or other functions can be used to satisfy training requirements. Training will be documented in the AF Form 623a On-the-Job Training Record, a computer generated Ancillary Training Record, or an approved automated system. Unit Security Assistants or unit-appointed training personnel should work with the ISS to ensure they have current training materials

4.6.3. Unit Commander's may require personnel pass a SET test before granting unescorted entry to a restricted area. Unit Commander's, based upon the recommendations of Security Assistants and unit-appointed training personnel, will determine unit testing requirements. Unit Security Assistants and unit-appointed training personnel may coordinate with the ISS, unit training sections, and standardization and evaluation sections to develop a test bank of written questions tailored for their work center. **NOTE:** The ISS recommends a SET test to be between 25-30 questions, questions should be applicable to the unit's restricted area, and have a passing score of 80%.

4.6.4. In addition to the requirements listed in the basic instruction, the Unit Security Assistants or unit-appointed training personnel will include the following items:

- 4.6.4.1. Local Force Protection conditions and how the threat applies to the individual.
- 4.6.4.2. Information from this manual and the 92 ARW Integrated Defense Plan concerning restricted area entry, controlled area entry and other pertinent installation specific security information.
- 4.6.4.3. Local duress code and Distance Recognition Code (DRC) procedures.
- 4.6.4.4. Locations and designations of protection level resources on the installation.
- 4.6.4.5. Security Reporting and Alerting System information.
- 4.6.4.6. HELPING HAND/COVERED WAGON reporting hotlines to BDOC
- 4.6.4.7. TERRORIST or crime reporting hotlines to the BDOC.
- 4.6.4.8. Escort procedures for restricted areas.
 - 4.6.4.8.1. Escort Official ratios for restricted areas will not exceed a 1 to 25 ratio and PL 1/PL 2 areas will not exceed a 1 to 5 ratio.
 - 4.6.4.8.2. Ensure those selected as escort officials attend Phase I training and Phase II. Security Assistants or unit appointed training personnel will document annual training.
 - 4.6.4.8.3. Brief escort officials on their responsibilities for ensuring all vehicles and hand-carried items are searched prior to entering/exiting restricted areas and controlled areas.
 - 4.6.4.8.4. Ensure all persons being escorted into restricted areas are positively controlled at all times and briefed using the escort briefing in [Figure 4.1](#).

Figure 4.1. Controlled/Restricted Areas Escort Briefing

“I am _____, your escort while in this area. You will remain with me or my designee and closely follow any directions given at all times while in this area. You will follow all orders/directions given by Security Forces. In the event of an emergency, you will immediately depart the area under my supervision, through the entry control point. This is the entry control point. If at any time you become separated from your escort, return directly to the entry control point. State to the entry controller your name and that you have become separated from your escort. If you will be operating a vehicle, I will ride with you. If that is not possible, I will follow you at a safe distance at all times within the area. When you depart the area, you will leave before me. This applies whether on foot or in a vehicle. Two person concept does/does not apply. You will not be part of the two person team. In case of emergency, you will be evacuated by _____. Evacuation point is _____. Do you have any questions?”

4.6.4.8.5. Ensure all personnel understand that Security Forces entry controllers will use at least one of the five supporting identification verification techniques, (Personal Recognition, Telephonic/Radio Verification, Entry Authority List, Signature/Credential Check, and Sign and Countersign) prior to allowing entry.

4.6.4.8.6. Ensure all personnel understand that temporary restricted areas only become active when PL resources are present.

4.6.4.8.7. Ensure all personnel understand that a “Free Zone” is an area within the restricted or controlled area when construction projects and similar activities make it inappropriate or impractical to apply normal circulation controls.

4.6.4.8.8. Ensure all personnel understand that Protection Level 4 resources include Arms, Ammunition & Explosives (AA&E), Funds, and Pharmaceuticals.

4.6.4.8.9. Ensure all personnel understand that AF Form 1199CD authenticators will be locally devised via a memorandum for Line Badge Authenticators.

4.6.4.8.10. Ensure all personnel understand that RABs will be secured completely out of sight when outside a restricted area. When worn, RABs will be displayed with the picture side exposed, on the outermost garment and above the waist at all times. The badge may be removed (but still in possession) when performing intake/exhaust inspections, or in the immediate vicinity of aircraft running engines.

4.7. SET Exercises:

4.7.1. Security Assistants and unit-appointed training personnel will conduct continuation training by planning, conducting, and evaluating detection exercises in restricted and controlled areas. These exercises are designed to determine the effectiveness of the installation security program in controlled and restricted areas. The IDC has established complete exercise guidelines in accordance with AFI 36-2646, *Security Forces Training and Standardization Evaluation Programs*. Additionally, the IDC has determined eight (8) exercises per year will be conducted based on local operational needs, security awareness, and trends.

4.7.2. The IDC has approved a GO/NO GO grading scale for use during SET exercises. See [Attachment 4](#). In addition, the IDC has established an incentive program for outstanding performers during SET exercises. Individuals singled out by the Security

Assistant or unit-appointed training personnel as outstanding performers will receive a one-day pass at the discretion of the unit commander.

4.7.3. If an exercise failure occurs, the affected unit commander will be notified of the failure and that a re-evaluation with a similar scenario will be conducted within 30-60 days. All personnel will be notified of the re-evaluation results and lessons learned.

4.7.4. Security Assistant or unit-appointed training personnel will track all SET exercises, annotating the time, date and location of all exercises. A formal report for all exercises, including failures will be submitted to the DFC and commander of the affected unit. Face-to-face briefings with supervisory personnel, phone calls or email notifications containing a brief summary of the scenario, personnel involved and the outcome of the exercise will be conducted. A log of SET exercises and their results will be maintained for a period of one year after closeout.

5. OBTAINING A RESTRICTED AREA BADGE.

5.1. A DD Form 577, Appointment/Termination Record-Authorized Signature, and a Designation of Issuing Official for Restricted Area Badges letter must be on file with Pass and Registration for security assistants and commanders before RABs may be issued. The DD 577 must be hand carried to Pass and Registration. If the Designation letter has a wet signature it must be hand carried to Pass and Registration, or if it has a digital signature it may be e-mailed to: 92 SFS/S5B Pass and Registration. When a commander or security assistant changes, these documents must be re-accomplished. A DD Form 577 and Designation letter must be on file for every commander in your chain of command, i.e., the 92 ARW/CC appoints each group commander and each group commander appoints their respective squadron commanders. The support squadron for their group is responsible for obtaining the 92 ARW/CC documentation. For those agencies that do not have commanders, 92 MSG/CC/CD is designated to sign the DD Form 577.

5.1.1. Complete the DD Form 577 (dated NOV 2014) as follows, referring to Figure 5-1 as an example:

5.1.1.1. Blocks 1 - 5, are self-explanatory. Note: If a security assistant is listed in block 1, the squadron commander will be in block 9. If a squadron commander is in block 1, then the group commander will be in block 9.

5.1.1.2. Block 6, check "Certifying Officer."

5.1.1.3. Block 7, for commanders state: "Authorized to complete Sections I,II,III, and IV (all columns) of the AF Form 2586. Authorized to sign for Restricted Areas X and XX." Commanders authorized to sign for Restricted Areas are identified in **Table 1** to Tab J to Appendix 2 to Annex C to 92 ARW Plan 31-1. Area coordinators for entry into areas other than those authorized for a particular unit are identified in **Table 1** to Tab A to Appendix 2 to Annex C to 92 ARW PLAN 31-1. Commanders grant unescorted entry only for personnel within their units, excluding themselves.

5.1.1.4. Block 7, for security assistants state: "Authorized to complete Sections I,II,III, and IV (columns 1,2, and 3) of the AF Form 2586."

5.1.1.5. Block 8, add: AFI 31-101, AMC SUP to AFI 31-101, 92 ARW PLAN 31-1, and FAFB Manual 31-104.

- 5.1.1.6. Blocks 9 - 12, self-explanatory.
- 5.1.1.7. Block 13, digitally sign.
- 5.1.1.8. Block 14, same as block 1.
- 5.1.1.9. Block 15, self-explanatory.
- 5.1.1.10. Block 16a, digitally sign.
- 5.1.1.11. Block 16b, requires original wet signature so after digitally signing the form, print and sign.
- 5.1.1.12. Blocks 19 – 21, leave blank.

5.2. Restricted Area Badges are issued via an electronic AF IMT 2586, Unescorted Entry Authorization Certificate. The form must be completed electronically (except in the case of communications failure) and sent encrypted to the Pass and Registration organizational e-mail account at: 92 SFS/S5B Pass and Registration. During communications failure, the member receiving the RAB must hand carry the AF IMT 2586 to Pass and Registration and after RAB issue, the member will hand carry the completed form back to their security assistant. If the AF IMT 2586 was sent to the Pass and Registration mailbox and technical problems prevent the form from being processed electronically, Pass and Registration will print the form, complete it, and have the member return the printed form to their security assistant.

5.2.1. Complete the AF IMT 2586 as follows, referring to Figure 5-2 as an example:

- 5.2.1.1. Section I. Identification: Member's information.
- 5.2.1.2. Section II. Certification of Requesting Official: is the security assistant. Electronically sign.
- 5.2.1.3. Section III. Duty. This section must contain four separate lines containing the member's:

Figure 5.1. Duty Title

Duty Title:

Phase II Security Education Training (SET): Date

Escort Training: Date

Type of Security Investigation completed and date of investigation. (Example: "NAC, 01 Jan 2014")

Area 1 coordination through the Command Post requires the member's SSAN.

Note: Both training dates must be within one year of the security assistants' signature in section II. All personnel will receive escort training regardless of whether they will be designated as escort officials or not.

- 5.2.1.4. Section IV. Restricted/Controlled Area Coordination. Complete a separate line for each area as follows:
- 5.2.1.5. Column A, Area Number: area number requiring access to.

- 5.2.1.6. Column B, Escort Official: state Yes or No. (92 ARW/CC has delegated escort approval authority to squadron commanders. Squadron commanders may only grant escort authority to personnel from their unit.)
- 5.2.1.7. Column C, Type Area: either Restricted or Controlled.
- 5.2.1.8. Column D, Concur: commander marks Yes or No.
- 5.2.1.9. Column E, Date: ensure commander dates before they electronically sign. The AF Fm 2586 is valid for 60 days after the last approving official's signature.
- 5.2.1.10. Column F, Coordinating/Approving Official's Signature: commander electronically signs each area.
- 5.2.1.11. Section V, Restricted/Controlled Area Badge Issue: leave blank.
- 5.2.2. Upon RAB issue, Pass and Registration will securely e-mail the security assistant the completed electronic AF IMT 2586. Print a copy for your files and store the electronic form in your electronic file plan, if you have one.
- 5.2.3. Per AFRIMS, T 31-08 R03.00, AF IMT 2586's must be maintained for two years after the RAB is destroyed.
- 5.3. Restricted Area Badge (RAB) Update Procedures. Changes cannot be made to an electronically signed AF IMT 2586, therefore, any updates to add or delete an area, add or delete an escort official or change a name, physical feature, correct erroneous information, etc., requires a new AF IMT 2586.
- 5.4. Permanent Change of Station (PCS) Procedures. Personnel are required to out-process Pass and Registration to turn in their RAB when they PCS. Members must obtain their AF IMT 2586 from their security assistant and bring it with their RAB to Pass and Registration. Pass and Registration will retrieve the RAB and annotate the AF IMT 2586 with the member's status and date of RAB turn-in. Member is required to bring the AF IMT 2586 back to their security assistant for filing.
- 5.5. Permanent Change of Assignment (PCA) Procedures. Individuals that PCA out of their Group need to out-process their losing unit and Pass and Registration as identified above for PCS's. If the gaining unit requires the member to have a RAB then the new security assistant needs to initiate a new AF IMT 2586.
- 5.5.1. Individuals that PCA within their Group do not need to out-process Pass and Registration but must out-process their losing unit. The losing security assistant must transfer the member's AF IMT 2586 to the gaining security assistant and notify Pass and Registration so the member's unit can be updated on the MRABL.
- 5.6. Stolen Restricted Area Badge Procedures. If a member has their RAB stolen they must report it to the Security Forces Desk Sergeant at Bldg. 2071 and accomplish an AF IMT 1168, Statement of Suspect/Witness/Complainant. The member will obtain a copy of the AF IMT 1168 and deliver it to their Security Assistant for inclusion with the investigation report.
- 5.6.1. Lost Restricted Area Badge Procedures. Immediately report it to Pass and Registration. Have the member complete an AF IMT 1168 (not with Security Forces) for inclusion in your investigation report. Unit commanders must complete a letter of investigation explaining the loss circumstances and authorizing re-issue of the RAB, if

needed. Security Assistants must also sign this letter. Commanders must ensure extensive investigations are conducted prior to authorizing re-issue of the RAB.

5.6.2. Security Assistants will forward to Pass and Registration the commander's investigation letter, a copy of the member's AF IMT 1168, and the AF IMT 2586 used to issue the lost or stolen badge.

5.6.3. If the member requires a new RAB, then a new AF IMT 2586 must be completed according to 5.2. above.

5.7. Quarterly Reviews. Security Assistants must conduct a quarterly review to ensure all designation letters and DD FM 577's are current. Each quarter, Pass and Registration will send Security Assistants a Quarterly Review Letter with a suspense date. Failure to return the letter by the suspense date will result in an administrative hold on issuing badges until the letter is received.

5.8. New Security Assistant Audit. It is highly recommended you conduct an audit of your AF IMT 2586's against your unit's Master Restricted Area Badge Listing (MRABL) upon assuming duties as a security assistant. Every individual listed on the MRABL must have an AF IMT 2586 on file. Ensure the old security assistant fixes any discrepancies or you will have to.

5.9. Annual Validations and Inventories. Annually (no specific cutoff), the commander must validate all personnel's need to access restricted areas. The security assistant must document this validation via an official memorandum which is kept in the security assistant's files. Pass and Registration does not require this letter. Additionally, new commanders must conduct this validation within 90 days of assuming command and annually thereafter.

5.9.1. Annual RAB inventories must be conducted in January. Pass and Registration will send security assistants a current MRABL and a RAB Inventory Letter template to certify the results. Pass and Registration must receive the inventory letter results by 31 January. This is a physical hands-on inventory, not a paperwork review.

5.10. Adverse Actions. Security assistants must immediately retrieve RABs from individuals undergoing adverse actions. Security assistants hold on to the badge until the unit commander determines whether or not the member gets the RAB back. If the member will not get the RAB back then the security assistant must bring the RAB and AF IMT 2586 to Pass and Registration for turn-in.

5.11. Master Restricted Area Badge Listing. The MRABL identifies all personnel assigned by squadron. MRABL's will be provided to security assistants via encrypted e-mail upon request.

5.12. Office Hours. RABs are issued at the 92 SFS Pass and Registration section from 0730-1545 hours, Monday through Friday. Personnel must be in uniform and IAW AFI 36-2903 when requesting badges. Turn-in for deletion of RABs will be done no later than 1600 hours.

5.13. Wear of the Restricted Area Badge. The security assistant must brief all personnel issued a RAB on proper wear and placement. RABs will be secured completely out of sight when outside a restricted area. When worn, RABs will be displayed with the picture side exposed, on the outermost garment and above the waist at all times. The badge may be removed (but still in possession) when performing intake/exhaust inspections, or in the immediate vicinity of aircraft running engines.

Figure 5.2. Sample DD Form 577.

APPOINTMENT/TERMINATION RECORD - AUTHORIZED SIGNATURE (Read Privacy Act Statement and Instructions before completing form.)		
PRIVACY ACT STATEMENT		
<p>AUTHORITY: E.O. 9397, 31 U.S.C. Sections 3325, 3528, DoDFMR, 7000.14-R, Vol. 5. PRINCIPAL PURPOSE(S): To maintain a record of appointment and termination of appointment of persons to any of the positions listed in Item 6, and to identify the duties associated with this appointment. SORN T1300 (http://dpclo.defense.gov/Privacy/SORNs/index/DoDComponentArticleView/tabid/7489/Article/623561300.aspx) ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U.S.C Section 552a(b) of the Privacy Act of 1974, as amended. It may also be disclosed outside of the Department of Defense (DoD) to the Federal Reserve Banks to verify authority of the appointed individuals to issue Treasury checks. In addition, other Federal, State and local government agencies, which have identified a need to know, may obtain this information for the purpose(s) identified in the DoD Blanket Routine Uses published at: http://dpclo.defense.gov/Privacy/SORNs/index/BlanketRoutineUses.aspx. DISCLOSURE: Voluntary; however, failure to provide the requested information may preclude appointments.</p>		
SECTION I - APPOINTEE		
1. NAME (First, Middle Initial, Last and Rank or Grade) Sq CC or Sec Asst	2. DoD ID NUMBER on CAC card	3. TITLE Commander or Security Assistant
4. DOD COMPONENT/ORGANIZATION USAF	5. ADDRESS (Include Zip Code, email address, and telephone number with area code and DSN) Squadron/Office Symbol Phone Number	
6. POSITION TO WHICH APPOINTED (X appropriate box - one only. Checking more than one invalidates the appointment.)		
<input type="checkbox"/> DISBURSING OFFICER: DSSN _____	<input type="checkbox"/> CASHIER	<input type="checkbox"/> CHANGE FUND CUSTODIAN
<input type="checkbox"/> DEPUTY DISBURSING OFFICER: DSSN _____	<input type="checkbox"/> PAYING AGENT	<input type="checkbox"/> IMPREST FUND CASHIER
<input checked="" type="checkbox"/> CERTIFYING OFFICER	<input type="checkbox"/> COLLECTIONS AGENT	<input type="checkbox"/> SAFEKEEPING CUSTODIAN
<input type="checkbox"/> DEPARTMENTAL ACCOUNTABLE OFFICIAL	<input type="checkbox"/> DISBURSING AGENT	<input type="checkbox"/> ASSISTANT SAFEKEEPING CUSTODIAN
7. YOU ARE APPOINTED TO SERVE IN THE POSITION IDENTIFIED IN ITEM 6. YOUR RESPONSIBILITIES INCLUDE:		
FOR COMMANDERS STATE: "Authorized to complete Sections I, II, III, and IV (all columns) of the AF Fm 2586. Authorized to sign for Restricted Areas X and XX."		
FOR SECURITY ASSISTANTS STATE: "Authorized to complete Sections I, II, III, and IV (columns 1, 2, and 3) of the AF Fm 2586."		
8. REVIEW AND ADHERE TO THE FOLLOWING PUBLICATION(S) NEEDED TO ADEQUATELY PERFORM YOUR ASSIGNED DUTIES: AFI 31-101, AMC SUP to AFI 31-101, 92 ARW PLAN 31-1, and FAFB Manual 31-104		
SECTION II - APPOINTING AUTHORITY		
9. NAME (First, Middle Initial, Last) Gp CC if for Sq CC; Sq CC if for Sec Asst	10. TITLE Commander	11. DOD COMPONENT/ORGANIZATION Squadron
12. DATE (YYYYMMDD)	13. SIGNATURE	
SECTION III - APPOINTEE ACKNOWLEDGEMENT		
I acknowledge and accept the position and responsibilities defined above. I understand that I am strictly liable to the United States for all public funds or payment certification, as appropriate, under my control. I have been counseled on my pecuniary liability applicable to this appointment and have been given written operating instructions. I certify that my official signature is shown in item 16 below.		
14. PRINTED NAME (First, Middle Initial, Last) Block I Name: Digi sign, print, sign, hand carry	15. DATE (YYYYMMDD) (Not earlier than date in item 12 or 13)	
16.a. DIGITAL SIGNATURE	16.b. MANUAL SIGNATURE	
SECTION IV - APPOINTMENT TERMINATION		
The appointment of the individual named above is hereby revoked.	17. DATE (YYYYMMDD)	18. APPOINTEE INITIALS
19. NAME OF APPOINTING AUTHORITY	20. TITLE	21. APPOINTING AUTHORITY SIGNATURE

Figure 5.3. Instructions for completing DD Form 577.

INSTRUCTIONS FOR COMPLETING APPOINTMENT/TERMINATION RECORD - AUTHORIZED SIGNATURE	
Use this form to:	
1.	Appoint disbursing officers and their agents, e.g., deputy disbursing officers, disbursing agents, paying agents, cashiers, imprest fund cashiers, change fund custodians, and collection agents.
2.	Appoint certifying officers. Certifying officers are those individuals, military or civilian, designated to attest to the correctness of statements, facts, accounts, and amounts appearing on a voucher for payment.
3.	Appoint departmental officials. Departmental officials are those individuals, military or civilian, who are designated in writing and are not otherwise accountable under applicable law, who provide source information, data or service on which a certifying officer relies when certifying vouchers as correct and proper for payment.
4.	Appoint safekeeping custodians or assistants. Appointees to these positions are not subject to pecuniary liability.
5.	Governing guidance is in the Department of Defense Financial Management Regulation, Volume 5 (Disbursing Policy).
SECTION I.	
1.	Enter the Appointee's name and rank or grade.
2.	Enter the Appointee's 10-digit DoD Identification Number.
3.	Enter the Appointee's title.
4. - 5.	Enter the name, complete address (to include e-mail address), and telephone number (include DSN when available) of the DoD Component or activity to which appointed.
6.	Mark X in the appropriate box to indicate the duty the appointee will perform (select only one). If appointing a disbursing officer or deputy disbursing officer, enter the appropriate DSSN in the space provided.
7.	The appointing authority identifies the types of payments affected, but need only be specific as he or she considers necessary, and may include any other pertinent, applicable information (e.g., system involved).
8.	List all publications the Appointee must review and follow in order to adequately fulfill the requirements of the appointment.
SECTION II.	
9. - 12.	Enter the appointing authority's name, title, DoD Component/Organization location, and date signed.
13.	The appointing authority must enter his or her manual or digital signature. If signature is digital, completing item 12 is not required since the digital signature includes the date; enter only after completion of items 1 through 11, as this signature will "lock" those items.
SECTION III.	
14. - 16.	The appointee enters his or her name and digital (16a) or manual (16b) signature, or both, depending on type(s) of signature(s) to be employed, in the appropriate spaces. If the signature is manual (16b), complete item 15, but if the signature is ONLY digital (16a), completing item 15 is not required since the digital signature includes the date. If the appointee enters both manual and digital signatures, the dates in items 15 and 16a must match. The date in item 15 (or 16a if signed digitally) cannot be earlier than the date in item 12 or 13. The appointment is effective on the date of acceptance by the appointee, and is not in force without his or her acknowledgement.
SECTION IV.	
Completing this section terminates the original appointment. If partial authority is to be retained, complete a new DD Form 577.	
17.	Enter the date the termination is effective. Completion of this item is not required if item 21 is signed digitally, since the electronic signature includes the date.
18.	The appointee initials in the space provided acknowledging revocation of the appointment.
19. - 21.	The appointing authority enters his or her name, title and signature (which may be digital) in the spaces provided.

Figure 5.4. Sample AF Form 2586.

UNESCORTED ENTRY AUTHORIZATION CERTIFICATE						
PRIVACY ACT STATEMENT						
<small>AUTHORITY: 10 U.S.C. 9013, Secretary of the Air Force, 44 U.S.C. 3101, Implemented by Air Force Instruction 31-101, Integrated Defense.</small>						
<small>PRINCIPLE PURPOSE(S): To record personal information on an individual whose duty performance requires entry into Air Force restricted and controlled areas in order to coordinate with the appropriate official and determine when and what type of entry credential to use. Control number is used for individual identification. (Must be from government-issued ID such as CAC, driver license, passport, etc.)</small>						
<small>ROUTINE USE(S): In addition to those disclosures generally under 5 U.S.C. 552a(f) of the Privacy Act, these records or information contained therein may specifically be disclosed to appropriate Federal agencies for appropriate action, Congressional representatives, Contractors, Law Enforcement (Investigations), and/or the Department of Justice. Information may also be provided for Breach Mitigation and Notification and/or to the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.</small>						
<small>DISCLOSURE: Disclosure is voluntary however, failure to disclose required information will result in not being allowed entry into these areas.</small>						
<small>SYSTEM OF RECORDS NOTICE: F031 AF OF B Security Forces Management Information System http://pcid.defense.gov/Privacy/SOR/indexDOC-wide-SORN-Article-View/Article/5697154031-af-of-b/</small>						
I. IDENTIFICATION						
NAME (Last, First, Middle Initial)				GRADE	CONTROL NUMBER	
DOE, JOHN A.				ENL	0123456789	
ORGANIZATION AND UNIT, OR FIRM			HEIGHT	WEIGHT	COLOR EYES	COLOR HAIR
92 SFS			70"	165	HZL	BRN
CITIZENSHIP (Check One) <input checked="" type="checkbox"/> US CITIZEN <input type="checkbox"/> ALIEN IMMIGRANT <input type="checkbox"/> NON-US NATIONAL						
II. CERTIFICATION OF REQUESTING OFFICIAL						
<small>I certify that the individual whose name appears above has been the subject of a favorable investigation which meets the requirements of AFIs 31-101 and AFI 16-1405, when applicable, for unescorted entry into restricted or controlled areas. I further certify, in the event the above named individual is a non-US national, that no US nationals can be made available to fill this position during the period indicated above, and that the granting of unescorted entry represents an exceptional requirement essential to the proper execution of the Command's mission. Such unescorted entry will not infringe upon the prohibited duties outlined in AFPD 31-series directives, and is clearly consistent with the interest of national security.</small>						
NAME, GRADE AND TITLE (Typed)				SIGNATURE	DATE	
JANE A. DOE, Security Assistant, 92 SFS				Signature	6 MAY 21	
III. DUTY						
<small>(Describe duties that require unescorted entry into the areas indicated)</small>						
Duty Title:						
Phase II, Security Education Training (SET): Date						
Escort Training: Date (Everyone must be trained even if they won't escort.)						
Type of Security Investigation completed and date of investigation: (Example: "T3, 29 Mar 18").						
SSAN if Area 1 coordination is needed through the WCP.						
IV. RESTRICTED/CONTROLLED AREA COORDINATION						
AREA NUMBERS	ESCORT OFFICIAL	TYPE AREA	CONCUR		DATE	COORDINATING/APPROVING OFFICIAL'S SIGNATURE
			YES	NO		
5	N	RESTRICTED	Y			Signature
16	Y	CONTROLLED	Y			Signature
						Signature
						Signature
						Signature
						Signature
						Signature

Figure 5.5. Reverse Side of Sample AF Form 2586.

IV. RESTRICTED/CONTROLLED AREA COORDINATION						
AREA NUMBERS	ESCORT OFFICIAL	TYPE AREA	CONCUR		DATE	COORDINATING/APPROVING OFFICIAL'S SIGNATURE
			YES	NO		
						Signature
						Signature
						Signature
						Signature
						Signature

V. RESTRICTED/CONTROLLED AREA BADGE ISSUE				
TRANSACTION	FORM TYPE	DATE	CARD NUMBER	BADGE NUMBER
BASIC BADGE				
			BADGE ISSUING OFFICIAL (Type, Sign) Signature	APPLICANT RECEIPT OF BADGE Signature
EXCHANGE BADGE #1				
			BADGE ISSUING OFFICIAL (Type, Sign) Signature	APPLICANT RECEIPT OF BADGE Signature
EXCHANGE BADGE #2				
			BADGE ISSUING OFFICIAL (Type, Sign) Signature	APPLICANT RECEIPT OF BADGE Signature
REISSUE #1				
			BADGE ISSUING OFFICIAL (Type, Sign) Signature	APPLICANT RECEIPT OF BADGE Signature
REISSUE #2				
			BADGE ISSUING OFFICIAL (Type, Sign) Signature	APPLICANT RECEIPT OF BADGE Signature

REMARKS

Figure 5.6. Page 3 of Sample AF Form 2586.

1. Completing AF Form 2586. The individual's unit commander or designee completes Sections I, II and III, and Columns 1, 2 and 3 of Section IV. An electronic signature of the unit commander or designee in Section II certifies that all records were reviewed and contain no disqualifying information. **NOTE:** An electronically signed AF Form 2586 will be used as the primary form for Restricted Area Badge (RAB) issuance, unless such processing is unsustainable, impractical (e.g. installation-wide mass reissue) or restricted by computer/network connections. In such instances, the provisions of paragraph 1.4. will apply. AF Forms 2586 will be sent to the RAB Issuing Office via digitally encrypted means (digitally encrypted email, SharePoint, etc.) so the electronic form can be verified.

1.1. Approving officials complete the applicable portions of Section IV. **NOTE:** The installation commander designates approving officials for each area by naming their positions in the Integrated Defense Plan (IDP). Installation commanders may designate SF unit commanders as approving officials for SF personnel. Approving officials may designate other personnel as designees to sign on behalf of the approving official.

1.2. All personnel issued a RAB will be trained as an escort official IAW AFI 31-101. No additional "approved escort official" markings are required. MAJCOMs may supplement this requirement IAW paragraph 1.2.1.

1.2.1. If the MAJCOM or installation commander chooses to be more selective (e.g. not directing all personnel with a RAB to be an Escort Official), they will designate Escort Officials by marking the Escort Official Block in Section IV of the AF Form 2586 as well as placing an "E" next to the appropriate area on the AF Form 1199 series badge. Escort Official training will be documented in the remarks section of the AF Form 2586 IAW paragraph 1.2.2.

1.2.2. Unit security managers or persons designated by the unit commanders will document initial escort training in the "remarks" section of the AF Form 2586 during initial RAB issue. Recurring escort training will be conducted annually and documented locally.

1.3. Approving officials electronically sign in Section IV.

1.4. For electronic signatures, the signature verification form should include the individual's 10-digit Electronic Data Interchange Personal Identifier (EDIPI) for comparison. For printed versions of the form, use a signature verification (same signature) for those persons signing the form. Signature verification forms should contain both EDIPI and written signatures to ensure either version of the form can be used as necessary. Compare the signature on the AF Form 2586 with the signature verification form.

1.5. To protect personal identity, the Control Number from a government issued identification card with picture, such as CAC, driver's license, passport, etc, will be used to verify the identity of the individual requesting issuance of a RAB. Pictured identification other than a CAC will be used only when the person does not have a CAC. When using the CAC, the DoD Identification Number will be used. MAJCOMs may authorize the use of a control number from host nation government issued identification with picture at OCONUS locations and CONUS bases where foreign nationals require RABs. The Control Number utilized on the RAB will be the control number used when individuals are placed on an Entry Authority List.

AF IMT 2586, 20200713, (PAGE 3)

6. FREE ZONE GUIDE

6.1. Restricted Area Free Zone.

6.1.1. Establishment of a Free Zone requires certain levels of approval and should only be considered for projects lasting more than two weeks. Escorts are highly encouraged for work requiring less than 2 weeks in Controlled and Restricted Areas. The IDC Chairman is the Free Zone approval authority for all PL1-3 Restricted Area. Free zone are not required for Controlled Areas and access control is covered below. Free Zone establishment and concepts of operations for these areas must be carefully considered, fully staffed and approved in writing.

6.1.2. A Free Zone will be established IAW AFI 31-101 for projects exceeding two weeks.

6.1.2.1. Free Zone Request Procedures. The requesting agency will prepare the Free Zone Request via TMT. If TMT is unavailable, AF Form 1768, *Staff Summary Sheet* is optional. Approximately 30-days should be allowed for the entire process, from routine submission of the Free Zone request to the date of approval. This request process should begin far enough in advance so that it is completed at least seven days before the Free Zone is expected to begin.

6.1.2.2. The body of the TMT tasker (or AF Form 1768) will address the following items:

6.1.2.2.1. Identification of the sponsoring agency (end-user) for the Free Zone.

6.1.2.2.2. Identify the area and the reason for the Free Zone establishment.

6.1.2.2.3. Justify the need for a Free Zone versus providing escorts for the project.

6.1.2.2.4. Identify the work duration (dates) the Free Zone will be in effect.

6.1.2.2.5. Identify the work hours the Free Zone will be occupied.

6.1.2.2.6. For contracts, ensure to include in the statement of work that it will be the responsibility of the contractor to provide all materials except Restricted or Controlled Area signs to establish the free zone boundary, have it inspected by SFS and approved before any work can begin. This may require the sponsoring agency to provide escorts for the contractor until the free zone is established and approved by SFS. Some free zones may require painting specific markings on pavement.

6.1.2.2.7. Requesting agency may provide the free zone request package to 92 SFS/S5 for review prior to entering into TMT.

6.1.2.2.8. Attach a map, which identifies the entry point, Free Zone boundary, and (if required) the Free Zone corridor.

6.1.2.3. The TMT tasker (or AF Form 1768) will be routed for coordination/approval through the following agencies in the order listed:

6.1.2.3.1. 92 SFS/CC (Security Forces Commander) (Coord).

6.1.2.3.2. Group/CC that owns the area where the project will be performed (Coord).

6.1.2.3.3. 92 MSG/CCE (Mission Support Group Executive Officer) (Review)

6.1.2.3.4. 92 MSG/CC (Mission Support Group/Commander) (Coord).

6.1.2.3.5. 92 ARW/CCE (Air Refueling Wing/Wing Executive Officer) (Review).

6.1.2.36. 92 ARW/CV (Air Refueling Wing/Vice Commander) (Coord).

6.1.2.3.7. 92 ARW/CC (Air Refueling Wing/Commander) (Approve/Disapprove).

6.1.3. Actions After Coordination. The requesting agency will provide a complete copy of the package to 92 SFS/S5S (NCOIC, Installation Security) for restricted areas. NCOIC, Installation Security Section (92 SFS/S5S) must receive approved packages a minimum of seven calendar days prior to the Free Zone taking effect. This allows for sufficient time to coordinate with the contractor for establishment of the Free Zone boundary.

6.1.4. The organization or agency most directly associated with the project will maintain surveillance over the restricted area Free Zone and safe corridor boundary if the area is not segregated from the restricted area and must provide escorts where applicable. The escorts must provide immediate visual assessment (IVA) of the Free Zone boundary, and control entry/exit to the Free Zone area. **Note:** SF will not be used to conduct any of these actions.

6.1.5. The on-site superintendent must contact SFS BDOC (509-247-5493) and Airfield Management (509-247-5202) prior to opening the free zone each day. Notify both agencies again when they are ready to close the free zone. SF will dispatch a patrol to conduct a joint inspection with the superintendent to ensure the free zone is properly secured before departure.

6.2. Controlled Area Access

6.2.1. Free Zones are not required for access to controlled areas. The agency responsible for the project will develop an entry authority list (EAL) for the affected area and provide it to the controlled area Commander/Agency Chief for approval. Once signed by Commander/Agency Chief, it will be provided to 92 SFS/S5 or 92 SFS/S5C for authentication and distribution. Once the EAL is returned to the responsible agency, a copy will be provided to the contractor/visiting team who will maintain a copy on-site.

CASSIUS T. BENTLEY III, Colonel, USAF
Commander, 92d Air Refueling Wing

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References:***

92 ARW Integrated Defense Plan 31-1
AFI 16-1404, *Air Force Information Security Program*
AFI 31-101, *Integrated Defense*
AFI 31-118, *SF Standards and Procedures*

Prescribed Forms:

None.

Adopted Forms:

AF Form 847, *Recommendation for Change of Publication*
AF Form 1297, *Temporary Issue Receipt*
AF Form 2586, *Unescorted Entry Authorization Certificate*
DD Form 577, *Appointment/Termination Record-Authorized Signature*

Abbreviations and Acronyms

AA&E—Arms, Ammunition, & Explosives
ADAPT—Alcohol and Drug Abuse Prevention and Treatment
AFB—Air Force Base
AFJIS—Armed Forces Justice Information System
AFRIMS—Air Force Records Information Management System
ANG—Air National Guard
ARFC—Armed Forces Reserve Command
BDOC—Base Defense Operations Center
CA-CRL—Custodian Authorization Custody Receipt Listing
CAP—Citizens Awareness Program
CP—Crime Prevention
CPP—Crime Prevention Program
CPPM—Crime Prevention Program Manager
CPTED—Crime Prevention Through Environmental Design
DFC—Defense Force Commander
DoD—Department of Defense
FAFB—Fairchild Air Force Base

FOUO—For Official Use Only
ID—Integrated Defense
SET—Security Education Training
IDC—Integrated Defense Council
IDWG—Integrated Defense Working Group
IAW—In Accordance With
MRABL—Master Restricted Area Badge Listing
MOA—Memorandum of Agreement
MOU—Memorandum of Understanding
OPID—Operation ID
OPR—Office of Primary Responsibility
PCA—Permanent Change of Assignment
PCS—Permanent Change of Station
RAB—Restricted Area Badge
RDS—Records Disposition Schedule
SAV—Staff Assistance Visit
SCOPE—Sheriff’s Community Oriented Policing Effort
TSCG—Traffic Safety Coordination Group
UCMJ—Uniformed Code of Military Justice

Attachment 2

PRIMARY SECURITY COORDINATOR LETTER

A2.1. Your unit commander or general manager should identify a primary and an alternate Primary Security Coordinator. The following is an example of the letter:

Figure A2.1. Sample Letter.

Letterhead

(Date)

MEMORANDUM FOR 92 SFS/S5L

FROM: (Owner/User Agency)

SUBJECT: Primary Security Coordinator Letter

1. The following personnel are identified as Primary Security Coordinators for (Unit/Agency). Primary Security Coordinators are responsible for disseminating pertinent resource protection/crime prevention information to unit's/agency's members and general security of the unit/agency for all resource protection/crime prevention issues.

RANK & NAME	DUTY PHONE
PRIMARY:	
ALTERNATE:	

2. Authority: AFI 31-101, *Integrated Defense* and AFI 31-118, *SF Standards and Procedures*.

3. Purpose: To manage, monitor, and represent program requirements for this organization.

4. Period: From this date until officially relieved of duty or released from this appointment.

5. Special Instructions: As required. The primary manager, monitor, or representative will maintain a continuity folder containing this appointment letter and all pertinent correspondence relating to this additional duty. A replacement will be trained by the primary and identified in writing by the commander thirty days prior to the PCS/PCA of the primary or alternate program manager, monitor, or representative.

Commander's/Manager's/authorized signature block

cc: 92 SFS/S5A
92 SFS/S5S
Each Individual

Attachment 3

SET SELF INSPECTION CHECKLIST

Figure A3.1. Sample SET SELF INSPECTION CHECKLIST.

Task: Unit Security Education Training Program			
1. Is Phase I, Orientation Training being accomplished as required IAW FAFB Manual 31-104? Conduct this training during indoctrination training to the installation. Unit Security Assistant distributes ID Smart Book, located on the SharePoint to new personnel. Members also attend FAFB Right Start for Phase One Briefing.	YE S	No	N/A
2. Does the Unit Security Assistant have the most current Security Education Training materials IAW FAFB Manual 31-104? A. Access to ISS SharePoint Site? https://eim.amc.af.mil/org/92sfs/S5/ID_Awareness/Lists/SET%20Materials/AllItems.aspx B. ID Smart Book? C. Up-to-date Training Materials? D. (If Applicable) Updated SET and escort tests? ****Unit Security Assistants maintains all current material.	YE S	No	N/A
3. The unit, as part of their ancillary training program, conducts Part II. Is Phase II, Continuation Training being accomplished as required IAW FAFB Manual 31-104? A. Do Unit Security Assistants conduct initial Escort Training? B. Annual Refresher Training? C. Certify those persons selected as escort officials? D. Is training recorded and maintained?	YE S	No	N/A
4. Does the Unit Security Assistant include the following topics in Phase II training IAW FAFB Manual 31-104? A. Information on threats to USAF protection level resources? B. Security procedures for restricted/controlled areas (i.e. circulation and entry control)? C. Duress words and authentication procedures? D. (If Applicable) Written knowledge tests?	YE S	No	N/A
5. Is documentation of Phase II training accomplished in the AF Form 623 On-the-Job Training Record, computer generated Ancillary Training Record, or on a locally devised form IAW FAFB Manual 31-104? (Excel/computer database is acceptable)	YE S	No	N/A

6. Is the Annual Training Report for Ancillary Security Education Training and Escort Official Training and applicable testing maintained by the Unit Security Assistant and available for review? IAW FAFB Manual 31-104?	YES S	No	N/A
7. Does the Unit Security Assistant maintain Security Education Training Program trends of high missed areas IAW FAFB Manual 31-104?	YES S	No	N/A
8. (If Applicable) Are written knowledge tests being administered as required and is this test tailored to the specific duties of their work centers IAW FAFB Manual 31-104?	YES S	No	N/A

Attachment 4

SAMPLE SET TRAINING EVALUATION CHECKLIST

Figure A4.1. Sample TEEO.

(TRAINING, EXERCISE, EVALUATION OUTLINE (TEEO))	
: _____	
SET EXERCISE SCENARIO WORKSHEET: # _____	
EVALUATOR (S): _____	DATE: _____
<p>1. GENERAL CONDITIONS: Tests the ability of personnel working in a restricted/controlled area to detect and react to exercise in-put an individual utilizing duress codes.</p> <p>2. PRIMARY TRAINING, EXERCISE, EVALUATION STANDARDS: To receive a mission ready rating, the person must complete all appropriate actions to detect, challenge, sound the alarm, control the suspect, and brief responding Security Forces. Additionally, the detector or the detector' control center mut have made timely notification to either the Flight line Security Patrol and/or the Base Defense Operations Center (BDOC).</p> <p>3. TRAINING, EXERCISE EVALUATION RESULTS: This is to test the individual's awareness on each task for this mission. Trainers or evaluators and exercise controllers will record other pertinent information on a separate sheet of paper. The overall proficiency rating for this mission is determined from the individual's performance on each task, the primary training and evaluation standards, and the evaluator's subjective judgment as to whether personnel would have been successful in a real-life situation. For each applicable task, the evaluator will assess performance using the following standards:</p> <p style="padding-left: 40px;">A. <u>GO</u> – Mission ready</p> <p style="padding-left: 40px;">B. <u>NO GO</u> – Not mission ready</p> <p>4. SUGGESTED SUPPORT REQUIREMENTS:</p> <p style="padding-left: 40px;">A. EVALUATOR DUTIES: The Evaluator(s) for this exercise may be the Installation Security Section or any designated representative. This exercise must be coordinated with the BDOC and/or CP to prevent confusion and/or interference with real world incidents. Furthermore, evaluators will be in position to exercise positive control throughout the scenario at the point where perpetrators and responding forces meet. The exercise will be terminated immediately if a potentially dangerous/unsafe situation exists.</p> <p style="padding-left: 40px;">B. PERPETRATORS: (An individual may be used)</p>	

C. EXERCISE INPUT CARDS: (Attached) Exercise cards will be made available as appropriate. The evaluator(s) will ensure the card recipients fully understand the exercise situation prior to initiation.

5. CONSIDERATIONS:

A. SAFETY REQUIREMENTS: Safety of personnel will be in the forefront of everyone's mind and stringently enforced at all times. **Again, this exercise will be immediately terminated if a potentially dangerous situation exists. Exercise Safety briefing will be accomplished.**

B. PROHIBITED PRACTICES: Any deviation from this Training, Exercise and evaluation Outline (TEEO) will result in the immediate termination of the exercise. At no time will perpetrators carry actual weapons. NOTE: Simulated weapons may be used in a controlled environment

C. EXERCISE COMMUNICATIONS: A communications capability will be maintained between exercise participants and evaluators. Selected evaluators will be equipped with radio communications. Clear text voice communications will be used at all times during the exercise. The advisement "EXERCISE" will precede and follow the initial exercise communication, for radio/telephone transmissions, and will be used frequently throughout the exercise. All responding personnel at the initiation of the exercise will acknowledge the presence of perpetrators.

D. CRITIQUE: A critique will be conducted upon termination of the exercise by the evaluator(s). A listing of discrepancies will be documented.

E. REFERENCES: AFI 36-2646, AFI 31-101, AFI 31-101 AMC_SUP1, AMCP 31-3, AMI 90-201, AMCSUP, para. 2.4.2

ASSIGNED RATING	NO GO	GO
DETECTION (TIMELINESS OF)		
CHALLENGE		
SOUND THE ALARM		
CONTROL THE PERPETRATOR (S)		
BRIEF RESPONDING SECURITY FORCES		
WERE PARTICIPANTS WEARING RABs		
WAS EFFECTED PURGED		
SAFETY		
OTHER		

Attachment 5

SECURITY EDUCATION TRAINING (SET) EXERCISE SAFETY BRIEFING

Figure A5.1. Sample SET Briefing.

ITEM #	BRIEFING ITEM	ACTION COMPLETED
1	A) INTRODUCE YOURSELF AND BRIEF YOUR CALL SIGN AND OTHER PERTINENT COMMUNICATIONS INFORMATION B) IDENTIFY THE EXERCISE CONTROL CENTER C) ASSIGN CALL SIGNS TO PERPETRATORS IF THEY HAVE RADIOS	
2	CONFIRM THE PRESENCE OF ALL EXERCISE PERPETRATORS	
3	CONFIRM THE PRESENCE OF EQUIPMENT ITEMS NEEDED A) UNIFORMS B) BOGUS CREDENTIALS C) RADIOS	
4	GIVE A DETAILED BRIEFING ON THE EXERCISE SCENARIO A) GIVE PERPETRATORS EXACT ACTIONS YOU WANT THEM TO TAKE B) IDENTIFY THE WORKCENTER OR AREA WHERE THE EXERCISE WILL BE CONDUCTED	
5	DISCUSS THE SPECIFIC OBJECTIVES OF THE SCENARIO A) DETAIL ANY ROOM ALLOWED FOR FREELANCING BY THE PERPETRATOR B) GIVE THE PERPETRATOR INSTRUCTIONS ON INFORMATION GATHERING (NAMES, UNIT AND ACTIONS TAKEN OR NOT TAKEN BY EXERCISE PARTICIPANTS)	
6	DISCUSS THE TIME LIMIT OF THE EXERCISE A) SPECIFIC TIMES SHOULD BE PLANNED AND ADHERED TO B) SET EXERCISES MAY BE DELAYED PENDING REAL-WORLD ACTIVITIES AND CONTINUED AS DEEMED NECESSARY	
7	DISCUSS A PLAN OF ACTION IF THE PERPETRATOR IS NOT DETECTED WITHIN THE TIME LIMIT A) DETERMINE TRAVEL ROUTES TO BE USED B) DETERMINE RALLY POINT	
8	GIVE DETAILED INSTRUCTIONS ON THE ACTION TO TAKE A) PERPETRATORS MUST OBEY INSTRUCTIONS B) PERPETRATORS MAY NOT COMMIT HOSTILE ACTS C) PERPETRATORS WILL NOT USE PHYSICAL VIOLENCE	
9	DISCUSS ACTIONS FOLLOWING THE EXERCISE	

Attachment 6
USER FEEDBACK

Figure A6.1. User Feedback

1. Users in the field are highly encouraged to submit comments on any DoD or AF level publication using AF Form 847, *Recommendation for Change of Publication*. Users may submit comments concerning any Fairchild AFB and Security Forces Publication including this document by using the template in this attachment and sending it to 92 SFS/S5X.

NOTE: Add any additional information on bond paper and include with this attachment. Please provide the following information as a minimum:

1.1. Full Name (Rank/First/Last):

1.2. Unit:

1.3. Address:

1.4. Phone (DSN or Commercial):

2. CONTENT:

2.1. Is the information provided accurate? If not, what needs to be updated?

2.2. Is this publication consistent with other AF documents?

2.3. Can this instruction be better organized for better understanding of the material presented?

2.4. Is the information provided useful? If not, how can we improve it?

3. Writing and Appearance.

3.1. Where does the publication need revision to make the writing more clear and concise? What words would you use?

3.2. Are the charts and figures clear and understandable? How would you revise them?

4. Recommended Urgent Change(s), if any:

5. Other Comments:

6. Send Responses to:

92 SFS/S5X (Plans)
2 East Arnold Street

Fairchild AFB, WA. 99011