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

FAIRCHILD AIR FORCE BASE
MANUAL

31-103

17 JUNE 2021

Security

ELECTRONIC SECURITY SYSTEM USER/MONITOR 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 31-103,\
26 Nov 18

Pages: 22

FAIRCHILDAFBMAN31-103 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 Uniform Code of Military Justice (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 AFB, both military and civilian, guard and reserve, as well as transient or personnel.

The Fairchild Air Force Base (AFB) Electronic Security System (ESS) User/Monitor Program Manual is being published by the Defense Force Commander in accordance with the requirements of the 92 ARW Integrated Defense Plan 31-1. This manual provides information and "how-to-guidance" for establishing and maintaining an effective ESS User/Monitor 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 DoD contractors as prescribed in AFI 16-1406, *Industrial Security Program* when contract performance depends on access to AF information.

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.

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 the Air Force (AF) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. 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 Form 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

1. GENERAL POLICY AND RESPONSIBILITIES.

1. 1. Wing Commanders Intent. Fairchild AFB Security Forces will implement the Electronic Security Systems (ESS) Program as the executive agency for ensuring the ESS Intrusion Detection Equipment (IDE), Card Access Control, and Video Surveillance (VS) processes and the interrelationships of the necessary agencies involved is provided for and periodically exercised in accordance with AFI 31-101 and AMC Supplement to AFI 31-101.

1.2. **Specific Responsibilities:** This section defines the specific responsibilities of each agency in the ESS planning process.

1.2.1. The 92 SFS/S5E [(ESS Manager) ESSM] will:

1.2.1.1. Manage all IDE, card access and video surveillance (VS) systems that terminate with the 92 SFS. Stand-alone systems may request assistance from the ESS Manager.

1.2.1.2. Issue and maintain all IDE, card access, and VS work orders that terminate with the 92 SFS.

1.2.1.3. Respond to alarmed, card access, VS areas for maintenance.

1.2.1.4. Maintain and troubleshoot the Buried Line Sensor (BLS), Global Aircrew Strategic Network Terminal (GASNT) and Closed Circuit Television (CCTV) in both the Christmas Tree Area (CTA) and the Aircraft Mass Parking Area (MPA).

1.2.1.5. Provide the 92 SFS alarm operators, owner user alarm training for those systems that terminate with the 92 SFS and stand-alone Advantor SF/Xi card access systems.

1.2.1.6. Upon request, conduct Intrusion Detection System (IDS), access control, and VS surveys.

1.2.1.7. Maintain alarm and access control activity records for a minimum of two years.

1.2.2. The 92 CS Commander will:

1.2.2.1. Provide communication support for IDS, card access, and VS systems and repair current communications related systems.

1.2.2.2. Maintain alarm phone lines free of noise at a maximum of -16db.

1.2.2.3. Maintain fiber and Ethernet communication lines for the alarmed areas, BLS, CCTVs, and VS.

1.2.2.4. Ensure Building 2447/Alternate Base Defense Operations Center (ABDOC) IDS and access control phone lines are operational.

1.2.3. The 92 Civil Engineering Squadron Commander will:

1.2.3.1. Ensure the 92 SFS/S5E is notified in advance (96-hour minimum) of all Fairchild AFB scheduled power outages. This will include dates, times, affected facilities, and expected loss of power. Compensatory plans to mitigate the power outage will be implemented (i.e., portable generator) and those plans will be submitted to 92 SFS/S5E to include a refueling plan.

1.2.3.2. Provide power for all IDE, card access, and VS power based equipment specifications originally approved through the CES work order system.

1.2.3.3. Troubleshoot power related issues for all BLS, GASNT, and other IDS, access control, and VS.

2. PROTECTION LEVEL (PL) 3 INTRUSION DETECTION SYSTEMS (IDS).

2.1. **PL 3 Areas.**

2.1.1. The CTA and the Aircraft MPA have BLS with CCTV Long Range Thermal Imagers (LTRI).

2.1.2. The 92 ARW Command Post GASNT have fence and gate sensors along with CCTVs.

2.2. **Managing IDS.** BDOC will notify the 92 SFS/S5E if any portion of the BLS, GASNT and/or CCTV fails. Failure of a particular sector/zone does not constitute posting or repositioning of resources.

2.3. **BLS and GASNT Alarm Testing.** The Electronic Security Equipment Master Installation Acceptance Test and Turnover Plan will be used for testing.

3. PROTECTION LEVEL (PL) 4 INTRUSION DETECTION SYSTEMS (IDS).

3.1. **PL 4 areas.** Will only be alarmed if directed by AFI 31-101 or the Integrated Defense Council (IDC). Owner/users are responsible for protection of the resource until it is relocated or the alarm is repaired if their PL 4 alarm system fails.

3.2. **Managing IDS.** The security forces manage IDE and duress systems.

4. ENDURA VIDEO SURVEILLANCE (VS).

4.1. **Endura VS.** The 92 CS is primarily responsible for the Endura Camera System and Network Storage Managers located at Buildings 2248, 1304, and all supporting equipment and software.

4.2. **92 CES/CC Responsibilities.**

4.2.1. Once notified, 92 CES shall troubleshoot all power supplies that directly or indirectly support Endura cameras, encoders, decoders, media converters, and routers.

4.2.2. When available, 92 CES shall provide various types of lifts and certified personnel to operate lifts for cameras.

4.2.3. 92 CES will train key SFS personnel to operate the lift, for instances when there are no operators available.

4.3. **92 CS/CC Responsibilities.**

4.3.1. 92 CS will replace defective inoperative Fiber Media Converters, fiber and Ethernet damaged and inoperative wires. The 92d CS will assist 92 SFS/ESS with Network Storage Managers and associated hard drives, and cables. Once all repairs have been corrected a performance test will occur.

4.3.2. 92 CS will ensure Endura System Manager(s) are in working order, receive software updates for both the Endura, Pelco Utilities, and other software regarding the Endura Camera System.

4.3.3. 92 CS will provide a minimum of two POCs to jointly work with the 92 SFS ESS Office regarding Endura related issues.

4.4. **92 SFS/S5E Responsibilities.**

4.4.1. ESS Manager will submit all Endura requests through the ESSWG and, if need be, to the IDWG and the IDC.

4.4.2. ESS Manager will issue, remove, or add Endura permission rights.

4.4.3. ESS Manager will maintain a listing of all Endura software loaded computers and pertinent information.

4.4.4. Not Used

4.4.5. ESS Manager will troubleshoot initial video feed loss to cameras and submit Remedy ticket(s).

4.4.6. ESS Manager will jointly work with the 92 CS and 92 CES to resolve camera issues.

4.4.7. ESS Manager will provide minor maintenance for cleaning camera lenses, removing insects, and ensuring dome and fixed camera covers are tight.

4.4.8. ESS Manager will ensuring proper camera naming conventions are made.

4.4.9. ESS Manager will report camera system(s) systematic issues to the ESSWG.

4.4.10. ESS Manager will ensure applicable cameras are recording.

4.4.11. ESSM will recommend establishing a priority system to repair cameras.

4.4.12. ESSM and/or the NCOIC will certify PL 4 and below camera surveillance systems.

5. UNIT REQUIREMENTS.

5.1. **Posting IDS Signs.** All facilities with an Intrusion Detections System (IDS) will post AFVA 31-232, Warning Sign. The entry into the Munitions Storage Area will be posted with this sign.

5.2. **IDS Definition.** Defined as having two levels of sensor protection. One level monitors entrance-ways, garage-style rollup doors, and hatches. The second level monitors the interior space of an area(s).

5.3. **Intrusion Detection Equipment (IDE) Definition.** A piece of alarm equipment that is part of an overall IDS, for example, a fixed or wireless duress, Balance Magnetic Switch (BMS), Passive Infrared (PIR), etc. If the area only has duress and the duress fails, posting is not required and relocating the resource is not required unless the owner unit commander deems necessary. If the resource is relocated, the owner user will inform Security Forces BDOC of the building, room number, and telephone number for the new area.

5.4. **Units with IDS.** Units will comply with the following:

5.4.1. Authorization to arm or disarm alarm. Specify by letter to 92 SFS/S5E who may arm or disarm alarm systems, point of contact for alarm problems and after duty hours notifications, and who may authenticate (refer to **attachment 3** for an example). Ensure the letter is current by updating the data each time the list of personnel authorized to arm and disarm changes. The applicable commander or his designated representative will identify a minimum of two individuals to be primary point of contacts (POC) for their alarmed area and ensure the ESS Office is informed. Digitally signed letters are acceptable. Area with duress only will specify by a letter to 92 SFS/S5E who is authorized to test and in the event an alarm is received authenticate (refer to **attachment 3** for an example). An authorized signature for duress only areas can be Section Chiefs, Superintendents, Section Managers, Operation Officers. If further clarification is needed contact 92 SFS Electronic Security Systems Manager 247-3424.

5.4.2. Facilities with card access control that is managed by the 92 SFS ESS Office will provide a letter (refer to attachment 4 for an example), or add individuals with access to the Alarm Authorization Letter, or other approved written (i.e., internal operating instructions)/verbal updates. Facilities that have access control will either produce a separate letter or Entry Authority Listing to ESS. Digitally signed letters are acceptable. An authorized signature for card access only areas can be Section Chiefs, Superintendents, Section Managers, Operation Officers".

5.4.3. When IDE fails or malfunctions, the activity user must provide continuous surveillance. Perform this surveillance until the repairs are completed or relocate the resources to an approved IDS facility. The owner/user must have a way to sound the alarm for security forces response to a theft attempt. The BDOC will contact the alarm technician to respond to repair problems with the Advantor alarm system.

5.4.4. Scheduled power outages that affects IDS (Duresses only not required) only facilities lasting more than four hours the owner user will provide the 92 SFS ESS office with a roster that contains rank, last and first name, assigned shift times (i.e., 0600 – 1400), and a telephone number that the individual can be reached.

5.4.5. Alarm Testing.

5.4.5.1. Before alarm testing occurs the owner user will authenticate with BDOC. BDOC will obtain the individual's last name. The BDOC will pass a number which corresponds to the individual's last name (initiating from the first letter to the last letter). For example: Last name is Zeppelin and the BDOC passes 2, Zeppelin will respond back with "Echo," the 2nd letter in their last name.

5.4.5.2. Second: The individual will respond back with their last four of their SSN after providing the first part of the authentication.

5.4.5.3. Scenario: Keypad lockout, the BDOC has notified you (Zeppelin) to authenticate. The BDOC passes you "3", you respond with "Papa, 1313."

5.4.6. Owner users that have either IDS or IDE are responsible for conducting initial, remedial, and as needed training for all authorized individuals. The POCs will record the training per their unit operating instruction and maintain the record for two years, one year active and one year inactive.

5.4.7. Owner users that fail to comply with either monthly and/or quarterly alarm testing procedures will submit an alarm test remedial action plan (refer to **attachment 6** for an example) within ten calendar days to the 92 SFS ESS Office. This plan will state what alarm test was missed and corrective action(s) that will be taken to ensure no repeat failures to conduct testing will occur. The plan will be signed by applicable branch superintendent and if warranted the commander.

5.4.8. The Arm/Disarm number and/or Personal Identification Number (PIN) shall be safeguarded and treated as "FOR OFFICIAL USE ONLY". If compromised, report it to 92 SFS ESS Office for issuance of a new Arm/Disarm number and/or PIN. Arm/Disarm number will not be shared with anyone, i.e., with subordinates, family, co-workers, etc. If investigation proves that a number was shared, the individual's arm/disarm rights will be removed and remedial training will occur. Prior to granting the individual's arm/disarm rights, the owner/users commander will submit a letter (refer to **attachment 5** for an example) stating that the individual has received remedial alarm training and submit it to 92 SFS ESS Office.

5.4.9. Alarm Testing.

5.4.9.1. Areas that have IDS will test once per calendar quarter (Jan – Mar, Apr – Jun, Jul – Sep, and Oct – Dec), unless these areas are armories and are required once per month. All hard duress (i.e., Fixed push button, wireless, and foot pedal) areas are required to be tested once per month. Soft duresses (i.e., Keypad and Card Reader Duresses) are required once per calendar quarter. Alarm tests, to include maintenance activities by the 92 SFS ESS Office, will be documented on the AF Form 2530, Alarm Test Record. See **Figure 5.1** for an example.

Figure 5.1. Alarm Test Record.

ALARM SYSTEM TEST RECORD

ACTIVITY			COMPONENT PARTS OF THE SYSTEM TESTED		
1 JAN - 31 DEC 2020			DURESSES		
ROOM/SECURITY CONTAINER NO.					
BLDG. 9000, 3RD FLOOR					
CUSTODIAN					
CHANTEL CADY					
DATE	TIME	INITIATED BY	RECEIVED BY	TEST RESULT	CORRECTIV E
31 JAN 2020	1100	CADY	SSGT BUSH	PASSED	N/A

5.4.9.2. Prior to all alarm tests, the alarm custodian will authenticate using paragraphs **5.4.5.1** through **5.4.5.3** Upon authentication, the alarm custodian will follow their Alarm Test Plan for each individual applicable alarmed area.

5.4.9.3. Per AFI 31-101, Paragraph 9.19.7. Conduct a minimum of three intrusion scenarios per likely avenue of approach in each sensor sector or zone. If a particular sensor and/or duress fail to activate, complete the test again to validate the results. If the sensor and/or duress fail again, immediately notify BDOC and 92 SFS ESS Office. Compensatory measures will be implemented depending on the criticality of the failed device. Testing scenarios are defined in the alarmed area's testing plans.

5.4.10. The 92 ESS Manager recommends the primary POC maintain an alarm continuity binder that contains the following:

5.4.10.1. Tab 1: Alarm Authorization Letter, additional letters regarding access control, Alarm Test Record (AF Form 2530), etc.

5.4.10.2. Tab 2: Alarm Test Plan.

5.4.10.3. Tab 3: Additional sensor training if not using the test plan as the training material. Copies of the training roster, roster will include last and first name, grade and/or titles for Civilians, date trained, who conducted the training and the individual's signature that were trained.

5.4.10.4. Tab 4: Email traffic that is pertinent and all sensor work orders.

5.4.11. Prior to issuing arm/disarm numbers, the individual will be trained by either the 92 SFS/S5E or the owner/user who has been trained. The individual who requests the number will provide 92 SFS/S5E with the date trained, by whom, arm/disarm, and PIN numbers.

5.5. **Funding.** Per AFI 31-101, Paragraph 9.7.3. Owner/users shall fund installation and sustainment of IDS for PL4 resources..

6. ALARM MALFUNCTIONS.

6.1. **Partial Failure.** A portion of the facility's IDE fails at the entrance or the interior. The 92 SFS ESS Office will make an assessment and respond accordingly.

6.2. **Major Malfunction.** A facility's IDE component failure that would allow an intruder to gain access without crossing a line of detection or detection capability. Either, primary or alternate annunciation equipment fails or malfunctions. The 92 SFS ESS Office will respond immediately, not to exceed 2 hours. The alarm contract technician will respond IAW AFI 31-101 Chapter 9, paragraph 9.22.3.2. and 9.22.3.3.

6.3. **Catastrophic Failure.** Occurs when the entire system or a major portion of it is inoperative. The 92 SFS ESS Office personnel will respond immediately, not to exceed 2 hours. The alarm contract technician will respond IAW AFI 31-101 Chapter 9, paragraph 9.22.3.2. and 9.22.3.3.

6.3.1. The Security Forces Controller will brief all patrols to conduct checks of alarmed facilities within their patrol zones in order of highest to lowest priority utilizing the priority response matrix.

6.3.2. The BDOC will contact the Security Forces Armory to verify status and instruct the on duty personnel to monitor the Security Forces Radio net and conduct status checks with the BDOC every 15 minutes during hours of darkness and increased FPCONs. Every 30 minutes otherwise.

6.3.3. The BDOC will recall alarmed facility alarm custodians to their facilities. Upon arrival, each custodian will be briefed that they are responsible for guarding the facility until the alarm is repaired or resources are relocated to a facility providing appropriate protection.

6.3.4. The BDOC will make notifications IAW Security Forces Notification Matrix. Upon termination, the BDOC will re-notify all appropriate agencies and matrix personnel.

6.3.5. If the alarm is to be inoperative for an extended period of time, coordination with Security Forces for periodic checks will need to be accomplished by owner/user personnel and approved on a case-by-case basis.

6.4. **IDE Fails or Malfunctions.** The activity user must provide continuous surveillance. Perform this surveillance until the repairs are completed or relocate the resources to an approved facility. The owner/user must have a way to sound the alarm for security forces response to a theft attempt. The BDOC will contact 92 SFS ESS Office to respond to repair problems with the alarm system.

7. ELECTRONIC SECURITY SYSTEMS WORKING GROUP (ESSWG).

7.1. **Purpose.** The Electronic Security Systems Working Group (ESSWG) manages the design, installation, modification, and maintenance of alarm systems. The communications squadron provides and maintains adequate telephone lines and computer support.

7.2. **Authority.** TAB D TO APPENDIX 4 TO ANNEX A TO 92 ARW PLAN 31-1: (*ELECTRONIC SECURITY SYSTEMS WORKING GROUP (ESSWG) CHARTER*).

7.3. **Acquisition or Modification of Alarm Systems, Surveillance Systems, and Automated Access Control Systems.** Requests for acquisition or modification including software updates of alarm, card access, or video surveillance system will be coordinated through ESSWG. Only controlled or Protection Level 1 – 3 areas require IDC approval before contract tendering. The ESSWG was formed and chartered to review and recommend approval of all alarms, duresses, access control systems, surveillance, and camera software. The ESSWG must be contacted in the initial planning phase of any construction, renovation or install (including temporary construction sites) projects requiring alarms, duresses, access control systems, cameras, or camera software. The OPR for the ESSWG is 92 SFS/S5E and can be reached at 247-3424. The ESSWG makes recommendations to the Integrated Defense Working Group (IDWG) and the Integrated Defense Council (IDC) for consideration concerning whether the system(s) should be approved or disapproved.

8. ALARM RESPONSE PROCEDURES.

8.1. **Purpose.** An armed robbery/attempted armed robbery or alarm activation has occurred on Fairchild AFB.

8.2. **Mission.** To ensure a swift response by Security Forces and other key personnel when an armed robbery/attempted armed robbery or alarm activation has occurred on Fairchild AFB.

8.3. **Armed Robbery/Attempted Armed Robbery.**

8.3.1. Concept of Operations: This threat clearly points out the need for well-planned procedures to ensure prompt, coordinated and effective actions by personnel from the activity concerned, responding Security Forces and other agencies required, in order to preclude the successful commission of such a crime.

8.3.2. Assumptions: When a robbery or attempted robbery occurs on Fairchild AFB, it must be assumed that the individual committing the act:

8.3.2.1. Has the capability to carry out the act.

8.3.2.2. Is armed unless conclusively proven otherwise.

8.3.2.3. Is in all probability under acute mental stress or is highly motivated and will not conform to a predictable or normal behavior pattern.

8.3.2.4. Is familiar with the immediate and surrounding geographical area and has planned an escape route.

8.3.3. Tasks and Responsibilities:

8.3.3.1. Each activity that stores, escorts or handles AA&E, funds or narcotics will ensure that:

8.3.3.1.1. Written instructions are developed detailing specific actions that personnel are to take in the event of a robbery or attempted robbery.

8.3.3.1.2. Personnel assigned or employed by the activity are trained and knowledgeable of these instructions.

8.3.3.1.3. All personnel assigned or employed by the activity are aware of actions to take in the event of a robbery or attempted robbery as outlined in this plan.

8.3.3.1.4. Personnel are familiar with the operation and location of communication equipment available for reporting such occurrences to the Security Forces.

8.3.3.1.5. Personnel know that robberies or attempted robberies are to be reported to the Security Forces via 911.

8.3.3.1.6. Personnel are familiar with the operation of installed silent duress alarm systems.

8.3.3.1.7. When notified of a robbery or attempted robbery at another facility (those actions may be simulated during exercises), personnel will:

8.3.3.1.7.1. Be observant of all personnel and their activity within their area.

8.3.3.1.7.2. Maintain on hand only those funds absolutely necessary.

8.3.3.2. The 92 SFS/CC will:

8.3.3.2.1. Maintain sufficient on-duty Security Forces to respond promptly to robbery/attempted robbery notifications.

8.3.3.2.2. Develop written procedures outlining actions and tactics to be employed by Security Forces personnel during an actual or attempted robbery.

8.3.3.2.3. Ensure all appropriate notifications are made.

8.3.3.2.4. Ensure the Security Forces desk blotter contains all necessary information and an Air Force Justice Information System (AFJIS) is accomplished.

8.3.3.2.5. Ensure Security Forces Investigations is notified and they assist in the investigation as needed.

8.3.3.3. Det 322, AFOSI will assist any other federal agency in the investigation of robberies or attempted robberies on Fairchild AFB where the other agency would have jurisdiction (i.e., base bank, credit union).

8.4. **Alarm Facility Procedures:**

8.4.1. Concept of Operations: In the event of an unannounced alarm activation or a mis-authentication of the code used in conjunction with opening/closing alarmed areas, BDOC will notify all posts and patrols of the incident and dispatch available patrols to the affected area. In the event of multiple alarm activations, dispatch patrols according to the SF response priority listing and the appropriate QRC. Terminate all routine radio communications.

8.4.1.1. The following base closure procedures apply:

8.4.1.1.1. When the alarm is from a firearms/munitions facility, BDOC duress, active duress, drug facilities or where an actual or attempted robbery has occurred at any facility, all outbound traffic will be stopped, inbound will utilize Stop/Check/Pass procedures.

8.4.1.1.2. When a description of the suspect is obtained, stop-check-pass of personnel/vehicles exiting the installation will be initiated at the installation entry points.

8.4.2. Arming and Disarming Procedures:

8.4.2.1. All personnel authorized to arm/disarm an alarmed facility and test all alarm points will be on a letter located within BDOC. This letter will originate from the unit's alarmed area supervisor and be authenticated by 92 SFS/S5E.

8.4.2.2. The Advantor alarm system operates off of a keypad entry and exit system. Arm/disarm numbers are assigned to personnel identified on the Alarmed Facility Access Authorization & Authentication letter (authenticated by 92 SFS/S5E). These numbers, which are individually assigned by a system administrator and unique to that person, will be used to arm and disarm facilities. Custodians may call BDOC before disarming and arming to prevent unauthorized alarm activations.

8.4.3. Alarm/False Alarms or Attempted Openings by Unauthorized Individuals:

8.4.3.1. The 92 SFS/BDOC will:

8.4.3.1.1. Notify all posts and patrols.

8.4.3.1.2. Dispatch the required patrols (minimum of 2 personnel) and direct patrols to secure the immediate area.

8.4.3.1.3. Follow base closure procedures outlined in **paragraph 8.4.1.1** above.

8.4.3.1.4. Contact the activity custodian where the alarm was received. During non-duty hours, the custodian will be directed to report to the senior Security Forces member at the scene.

8.4.3.1.5. If a false alarm, authenticate for termination with the senior on-scene Security Forces member.

8.4.3.1.6. Alarm and equipment malfunction(s) can only be determine by the ESS Office.

8.4.3.2. The senior Security Forces person on-scene will:

8.4.3.2.1. Direct the employment of patrols at the scene.

8.4.3.2.2. Keep BDOC informed of all events at the scene.

8.4.3.2.3. If the alarm was caused by a malfunction, authenticate for termination with BDOC and brief the custodian to implement appropriate security measures IAW AFI 31-101 and/or other applicable directives. If a guard must be armed, do so IAW AFI 31-101 and AFI 31-117.

8.5. **Authentication procedures:**

8.5.1. The authentication procedures are developed as a system to positively identify individuals requesting entry into alarmed areas and to ensure those individuals are not under duress at the time they request entry.

8.5.2. Authentication consists of two parts:

8.5.2.1. First: The BDOC will obtain the individual's last name. The BDOC will pass a number which corresponds to the individual's last name (initiating from the first letter to the last letter). For example: Last name is Zeppelin and the BDOC passes 2, Zeppelin will respond back with "Echo," the 2nd letter in his/her last name.

8.5.2.2. Second: The individual will respond back with their last four of their SSN after providing the first part of the authentication.

8.5.3. For example: Keypad lockout, the BDOC has notified you (Zeppelin) to authenticate. The BDOC passes you "3", you respond with "Papa, 1313."

8.5.4. Duress:

8.5.4.1. Personnel should be cautioned to respond with the correct letter if not under duress. All personnel while under duress will respond with a letter which does not match up with the number passed by the BDOC. An incorrect response is an indication the individual is under duress. The BDOC will not question an incorrect response to the number, but will immediately dispatch an armed security force response to the activity.

9. PROTECTION LEVEL 4 AND BELOW IDS, DURESS, AND ACCESS CONTROL SYSTEM CERTIFICATION.

9.1. **Purpose.** A newly installed or recertification IDS, Access Control System (ACS), or duress has been installed for either a PL 4 or non-PL rated area and requires test, acceptance, and certification with host, tenets, commercial, and other agencies associated to Fairchild AFB.

9.2. **Mission.** The authority to test, accept, and certified has been delegated to the 92 Security Forces Squadron (SFS) Electronic Security Systems Manager (ESSM) and/or the NCOIC.

9.3. **Testing.** Will be In Accordance With (IAW) Electronic Security Equipment (ESE) Master Installation Acceptance Test and Turnover Plan (ESE-TP-0023) and AFI 31-101.

9.3.1. IDS testing shall consist of the following when applicable.

9.3.1.1. Balance Magnetic Switch (BMS) and BMS tampers can be tested by either ESE-TP-0023 or using a strong magnet applied to the BMS switch. Over a period of a minimum of 10 years (Intrusion Detection Equipment replacement plan) damaging the BMS mounting holes will occur.

9.3.1.2. Passive Infrared (PIR) and tampers.

9.3.1.3. Keypads will be tested for arming, disarming, and sending a duress if applicable.

9.3.1.4. Alternating Current (AC) Power Loss.

9.3.1.5. All associated cabinet and junction box tampers.

9.3.1.6. Audio microphones.

9.3.2. ACS testing shall consist of the following when applicable.

9.3.2.1. Level I (Swipe only) and Level II (Swipe plus a personal identification number).

9.3.2.2. All associated cabinet, card reader, and junction box tampers.

9.3.2.3. Card reader duress(s).

9.3.2.4. The following proximity cards will be tested: Unknown card, restricted entry, invalid time, and access granted.

9.3.2.5. Request for Exit and/or push button request, and/or push bar/handle.

9.3.2.6. Emergency Override with or without audible siren. When override terminates as alarm point, validate alarm is generated when override is activated.

9.3.2.7. Magnetic and electric strikes lock.

9.3.2.8. AC power loss.

9.3.2.9. Magnetic locks will be tested with the fire alarms. Coordination will be made with the base fire inspectors.

9.3.3. Duress testing shall consist of the following when applicable.

9.3.3.1. Fixed duress(s).

9.3.3.2. Wireless duress(s).

9.3.3.3. Wireless receiver and cabinet tamper(s).

9.3.3.4. Low battery if applicable.

9.4. **Testing, acceptance, and certification.** Once testing is completed the 92 SFS/ESSM will prepare a memorandum stating acceptance, certification, and if there are discrepancies.

The ESSM will forward the memorandum to applicable involved parties. Regarding Sensitive Compartmentalized Information Facilities (SCIF), only the accreditation office can certify IDS and access control.

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

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-101, *Integrated Defense*, 6 July 2017 *Electronic Security Equipment (ESE) Master Installation Acceptance Test and Turnover Plan (ESE-TP-0023)*, 12 January 2017

Prescribed Forms

AF Form 2530, *Alarm Test Record*

AF Form 847, *Recommendation for Change of Publication*

Adopted Forms

None.

Abbreviations and Acronyms

ACS—Access Control System

AC—Alternating Current

AFB—Air Force Base

AFI—Air Force Instruction

AFJIS—Air Force Justice Information System

AMC—Air Mobility Command

BMS—Balance Magnetic Switch

BDOC—Base Defense Operations Center

BLS—Buried Line Sensor

CCTV—Closed Circuit Television

CTA—Christmas Tree Area

ECC—Emergency Communications Center

ESS—Electronic Security Systems

ESSM—Electronic Security Systems Manager

ESSWG—Electronic Security Systems Working Group

FPCON—Force Protection Condition

GASNT—Global Aircrew Strategic Network Terminal

IDE—Intrusion Detection Equipment

IDC—Integrated Defense Council

IDS—Intrusion Detection System

IDWG—Integrated Defense Working Group

LRTI—Long Range Thermal Imager

MAPA—Mass Aircraft Parking Area

OPR—Office of Primary Responsibility

PIR—Passive Infrared

PL—Protection Level

SFS—Security Forces Squadron

VS—Video Surveillance

Attachment 2

USER FEEDBACK

A2.1. 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.

Figure A2.1. User Feedback.

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

Full Name (Rank/First/Last):

Unit:

Address:

Phone (DSN or Commercial):

2. CONTENT:

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

Is this publication consistent with other AF documents?

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

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

Writing and Appearance.

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

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

Recommended Urgent Change(s), if any:

Other Comments:

Send Responses to:

92 SFS/S5X (Plans)
2 East Arnold Street
Fairchild AFB, WA. 99011

Attachment 3

SAMPLE ALARMED FACILITY ACCESS AUTHORIZATION LETTER

Figure A3.1. Sample Alarmed Facility Access Authorization Letter, Part 1.

DATE
MEMORANDUM FOR 92 SFS/S5E

FROM: Squadron & Office Symbol (i.e. 92 SFS/CC)

SUBJECT: (FOUO) Alarmed Facility Access Authorization and Authentication Letter

1. Name of facility: Alarmed facility name and Bldg. number: XXXX

2. Alarmed areas telephone number(s): (minimum of two numbers if possible)

3. Hours when Bldg. is secured: (i.e. 2000-0600, open 24 hours, Weekend Hours, etc.) This time needs to accurately reflect or Security Forces will call if the facility is disarmed outside the hours secured.

4. In case of emergency, contact the following personnel beginning with the first person listed (if you are unable to make contact continue to the next person):

NAME	RANK	HOME PHONE	*CELL PHONE (optional)*
Last, First, MI			
A minimum of 3-5 people is			
required			

5. The following personnel are authorized to arm/disarm/test the facility alarm:

NAME	RANK	LAST 4 SSN
Last, First, MI		XXXX

6. The authentication procedures are developed as a system to positively identify individuals requesting entry into alarmed areas and to ensure those individuals are not under duress at the time they request entry.

7. Authentication consists of two parts:

Figure A3.2. Sample Alarmed Facility Access Authorization Letter, Part 2.

7.1. First, the BDOC will obtain the individual's last name. The BDOC will pass a number which corresponds to the individual's last name (initiating from the first letter to the last letter). For example: Last name is Zeppelin and the BDOC passes 2, Zeppelin will respond back with "Echo," the 2nd letter in his/her last name.

7.2. Second: The individual will respond back with their last four of their SSN after providing the first part of the authentication.

7.3. Scenario: For example: Keypad lockout, the BDOC has notified you (Zeppelin) to authenticate. The BDOC passes you "3", you respond with "Papa, 1313.

8. Duress:

8.1. Personnel should be cautioned to respond with the correct letter if not under duress. All personnel while under duress will respond with a letter which does not match up with the number passed by the BDOC. An incorrect response is an indication the individual is under duress. The BDOC will not question an incorrect response to the number, but will immediately dispatch an armed security force response to the activity.

8.2. Should the Arm/Disarm number and/or Personal Identification Number (PIN) shall be safeguarded and treated as "FOR OFFICIAL USE ONLY". If compromised, you will report it to 92 SFS ESS Office for issuance of a new Arm/Disarm number and/or PIN. Arm/Disarm number will not be shared with anyone, i.e., with subordinates, family, co-workers, etc. If investigation proves that a number was shared the individual's arm/disarm rights will be removed and remedial training will occur. Prior to granting the individual's arm/disarm rights the owner user commander will submit a letter stating that the individual has received remedial alarm training and submit to 92 SFS ESS Office.

9. Final comments, all managers, custodians, etc., are responsible to ensure all individuals are authorized to arm/disarm/test are initially and every 90 days thereafter trained and the training is documented. This letter supersedes all previous letters making reference to the same subject. If you have any questions or comments, please contact 92 SFS/S5E at 247-3424.

Signature block of Squadron/Unit CC
Applicable Agency Manager
or designated Representative

92 SFS/S5E Signature
FOR OFFICIAL USE ONLY

Attachment 4

SAMPLE ALARMED FACILITY CARD ACCESS AUTHORIZATION LETTER

Figure A4.1. Sample Alarmed Facility Card Access Authorization Letter.

(DATE)
MEMORANDUM FOR 92 SFS/S5E

FROM: Squadron & Office Symbol (i.e. 92 SFS/CC)

SUBJECT: Card Access Authorization Letter

1. Name of facility: Card Access facility name and Bldg. number: XXXX

2. Room(s) XXX will be locked XX hours a day, X days a week.

3. The following personnel are authorized FPCON access based on the FPCON column. The highest FPCON indicates access to the area.

4. Alarmed areas telephone number(s): (minimum of two numbers if possible)

5. The following personnel are authorized to card access to the following area (i.e., if only one area is required list here, if multiple areas annotate the table below):

AREA	*NAME*	**RANK**	**CARD #**	**FPCON**	**SCHEDULE**
	Last, First, MI			A, B, C, D	Mon – Fri 0800 - 1600

6. Schedules grant permission rights for a specific time period, Monday to Friday, 0800 – 1700, or Monday, Wednesday, Friday, 0800 – 1000, 1400 – 1700, etc. My personnel will have 24 hours access as indicated by "24 hrs".

7. If the card is Personal Identification Number or the proximity card is compromised immediately report this information to your NCOIC, or Security Representative, and the 92 SFS/S5E, 247-3424.

Signature block of Section Chiefs,
Superintendents, Section Managers,
Operation Officers and
Applicable Agency Manager
or designated Representative

92 SFS/S5E Signature

Attachment 5

SAMPLE REMEDIAL ALARM TRAINING LETTER

Figure A5.1. Sample Remedial Alarm Training Letter.

DATE
MEMORANDUM FOR 92 SFS/S5E

FROM: Squadron & Office Symbol (i.e. 92 SFS/CC)

SUBJECT: Remedial Alarm Training Letter

1. The alarm incident (i.e., compromised alarm codes, failed to follow established alarm test procedures, arming, disarming procedures, etc.) that occurred on DD/Month/YYYY with Rank, Last Name, First has received the following training: Select the topics that were covered and delete the ones not covered, additional topics can be added

a. Monthly Alarm Test

b. Quarterly alarm Test to include Alarm Scenarios

c. Sensor Familiarization & Office Layout

d. Keypad Familiarization

e. Arming/Disarming Procedures

f. Card Reader Familiarization

g. Soft and Hard Duress Procedures

h. Authentication Procedures

2. Rank, Last Name is aware of his/her responsibilities, reinstate their arming/disarming and/or card access effective immediately.

3. If you have any questions referring to this incident please contact Rank, Last and First Name at 247-XXXX, Email Address.

Signature block of Squadron/Unit CC
Applicable Agency Manager
or designated Representative

Attachment 6

SAMPLE ALARMED TEST REMEDIAL ACTION PLAN

Figure A6.1. Sample Alarmed Test Remedial Action Plan.

DATE
MEMORANDUM FOR 92 SFS/S5E

FROM: Squadron & Office Symbol (i.e. 92 SFS/CC)

SUBJECT: Alarmed Test Remedial Action Plan

1. The Alarmed Area failed to comply with AFI 31-101, Integrated Defense Paragraph 9.19.1. and/or 9.19.4. by ensuring the quarterly Intrusion Detection System (IDS) was not tested during the X (i.e., 1st, 2nd, 3rd, 4th) Quarter of Year (i.e., 2016, etc.).

2. The following outlines the remedial actions that have been completed.

a. Rank, Last and First Name conducted refresher alarm test training to my staff (see attached roster for names) on DD MMM YY using the alarm test plan.

b. All quarterly alarm tests will be completed in the first month of each quarter.

c. All monthly duress test(s) will be completed if the first two week of each month.

3. If you have any questions please direct them to Rank, Last and First Name, Email Address, and duty phone XXX-XXXX.

Signature block of Squadron/Unit CC, or Agency Manager
or designated Representative