This instruction implements broader guidance found in DoD 5101.21-M-1, Sensitive Compartmented Information Administrative Security Manual, Air Force Policy Directive 31-1, Physical Security, and Air Force Instruction (AFI) 31-101, The Air Force Installation Security Program. It identifies local physical security procedures for the AF ISR Agency Restricted Area Complex located on Kelly Annex, Lackland Air Force Base, Texas. It also identifies local physical security procedures for the Building 2000/2007 Sensitive Compartmented Information Facility (SCIF). It applies to all occupants of Buildings 2000/2007 as well as all personnel entering the AF ISR Agency restricted area. NOTE: Cryptologic Systems Group (CPSG) personnel comply with the AF ISR Agency/CPSG Memorandum of Agreement. This instruction does not fully apply inside buildings 2028, 2049, 2058, and 2081 where separate internal physical security requirements exist. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional’s chain of command. Maintain records created as a result of prescribed processes IAW AFMAN 33-363, Management of Records, and dispose of them IAW the AF Records Disposition Schedule (RDS) at https://www.my.af.mil/gcss-af61a/afrims/afrims/. Contact supporting records managers as required.

SUMMARY OF CHANGES

This revision changes all references to Air Intelligence Agency to Air Force Surveillance and Reconnais-
sance Agency and specifies the number of personnel an escort official can observe.

2000/2007 is marked by solid wood entry doors. NOTE: Based on security clearance, entry credentials, and the unique configuration of the area, personnel may have unescorted entry into both the restricted area and SCIFs, to just the restricted area but not the SCIFs, or to neither the restricted area nor the SCIF.

2. Restricted Area Entry Control:

2.1. Entry Credentials. ECs are used to gain entry to the complex as well as aid internal circulation control within SCIFs. All personnel, regardless of rank, status, or age will be issued an EC for wear inside the complex. ECs are United States Government property and must be safeguarded at all times. Authorized ECs include: AFISRA Forms 325, 325C, 325CT, 325DV, 325F, 325FT, 325R, 325T, 325TY, 326, 326C, 326CT, 326DV, 326R, 326T, 332, 332DV, and 332E. Refer to AFI 31-101/AFISRASUP1 for detailed descriptions of authorized ECs.

2.1.1. EC Wear Requirements. ECs will be worn conspicuously below the neck, above the waist, and between the shoulders on the front of the outer-most garment with the front (photograph, “T”, “DV” or “Escort Required”) facing outward at all times while inside the restricted area complex. Upon exit, remove (do not display) and secure the EC. NOTE: Only ECs containing badge holder’s photographs may be taken outside the complex; all other badges—to include temporary, visitor, and DV—must remain inside the complex.

2.2. Entry Control Procedures. Entry into and exit from the complex is accomplished at one of two entry control points (ECPs): Building 2059 (adjacent to the CPSG area), and Building 2001 (primary Visitor Control facility). 37th Security Forces Squadron (SFS) personnel staff both ECPs. NOTE: SCIF entry control procedures for building 2000/2007 are addressed in paragraph 3.

2.2.1. Unescorted Entry into the Restricted Area. Personnel cleared for unescorted entry into the complex approach the ECP, present a valid EC, and present a second form of identification bearing a photograph—primarily the Common Access Card (CAC)—to the posted entry controller. The entry controller compares the photographs, physical characteristics, and all available identification data on the CAC (last six numbers of social security number, enlisted/officer/civilian/contractor data, etc.) with matching data on the EC prior to permitting unescorted entry.

2.2.1.1. Locally assigned personnel with Top Secret clearances and sensitive compartmented information (SCI) access, entry authority, and an appropriate EC (AFISRA Form 325, 325C, 325F, or 325R) are authorized unescorted entry throughout the restricted area and Buildings 2000/2007. NOTE: Entrance to interior rooms requires owner/user concurrence. Likewise, access into Buildings 2028, 2049, 2058, and 2081 require owner/user concurrence.

2.2.1.2. Visitors with Top Secret clearances and SCI access transmit clearance messages to AF ISR Agency/SOP for placement on the visitor roster. Upon arrival, visitors report to the ECP or Visitor Control for issue of AFISRA Form 325CT, 325DV, 325T or 325FT as applicable. These visitors are authorized unescorted entry to areas specified in paragraph 2.2.1.1. NOTE 1: These credentials do not leave the restricted area. NOTE 2: AF ISR Agency/DSP determines which visitors qualify for DV credentials.

2.2.1.3. Locally assigned personnel with Top Secret or Secret collateral clearances, entry authority, and appropriate EC (AFISRA Form 326, 326C, or 326R) are authorized unescorted entry to: all ground areas within the complex; the exterior of all facilities in the complex with the exception of Building 2028 warehouse; and, in Building 2000, the first floor hallway from the courtyard foyer to the center stairway to include the automatic teller machine (ATM),
Army and Air Force Exchange Service (AAFES) cafeteria, and the restrooms located in room L13 and L14.

2.2.1.4. Visitors with Top Secret clearances with SI access only, Top Secret or Secret collateral clearances transmit clearance messages via fax, memorandum, Automated Message Handling Service (AMHS), or Joint Personnel Adjudication System (JPAS) visit request to AF ISR Agency/SOP for placement on the visitor roster. Upon arrival, visitors report to the ECP or visitor control for issue of AFISRA Form 325TY, 326CT, 326DV, or 326T. These visitors are authorized unescorted entry to areas specified in paragraph 2.2.1.3. They must be escorted at all times while in the SCIF. **NOTE 1:** These credentials do not leave the restricted area. **NOTE 2:** AF ISR Agency/DSP determines which visitors qualify for DV credentials.

2.2.1.5. Personnel without security clearances, but with routine entry authority and appropriate EC (AFISRA Form 332) will proceed to and from their work areas. They are authorized unescorted entry to areas specified in paragraph 2.2.1.3.

2.2.2. Unescorted Exit Procedures. Locally assigned personnel with unescorted access to the restricted area approach the ECP and present a valid EC. The entry controller verifies badge validity prior to permitting exit. Visitors with unescorted access to the restricted area approach the same ECP they entered and present their visitor credential to the entry controller. Entry controllers retrieve ECs issued at their post; ECs issued at Visitor Control will be returned to Visitor Control.

2.2.3. Escorted Entry into the Restricted Area. Personnel requiring escorted entry must report to an ECP or Visitor Control to wait for their escort.

2.2.3.1. Escorted entry applies to individuals with official business to perform within the restricted area and who have not been granted unescorted entry. A trained and certified escort official—all personnel issued ECs with photographs except contractors (unless there is an E-1 printed on the contractor’s EC)—must escort these personnel throughout the duration of the visit.

2.2.3.2. Escorts will:

2.2.3.3. Be trained and certified annually.

2.2.3.4. At the restricted area boundary, meet and positively identify individuals requiring escorted entry.

2.2.3.5. Print all visitor and escort official point of contact information on the “Escort Required” sign-in log at the ECP. Visitor information includes name, rank/grade, organization or firm, social security number (last six digits only), and citizenship. Escort official information includes purpose of visit, point of contact (POC) name, escort official entry credential number, and time in. **NOTE:** Visitors must exit the restricted area at the same location they entered the area.

2.2.3.6. In the presence of the entry controller, recite the following visitor briefing to each person under escort. **NOTE:** Group briefings are permitted.

2.2.3.6.1. I am (state your name), your escort for this visit. Prior to entering the restricted area, I am required to brief you on security procedures and your responsibilities. While you are in the restricted area, you must be under escort by an authorized individual at all times. You must stay with your escort until you depart the area. You must visibly display
your AF ISR Agency entry credential on the front of your outermost garment—above the waist—at all times. If you are stopped or challenged by security forces, you must obey all instructions. Do you have any of the following items with you: personally owned photographic equipment, video equipment, audio recording equipment, computers and associated computer equipment, personal digital assistants, cellular phones, or two-way pagers? These are prohibited items (unless authorized in writing by AF ISR Agency/SO). You may not carry them into the restricted area. I am now required to search all handcarried items, vehicle(s), and equipment you plan to take into the restricted area. Be aware, while you are in the restricted area, your person and all your possessions are subject to inspection. Do you have any questions?

2.2.3.7. Maintain positive control and constant surveillance of escorted personnel at all times while in the restricted area. The number of individuals an escort official can escort at one time is based on the known trustworthiness of the visitors and the ability of the escort to have reasonable control of the visitors, but will not exceed 8 visitors.

2.2.4. Escorted Exit Procedures. Personnel under escort by a trained and certified escort official approach the same ECP they entered and present their visitor credential to the entry controller. The entry controller verifies badge validity prior to permitting exit. Entry controllers retrieve ECs issued at their post; ECs issued at Visitor Control will be returned to Visitor Control.

2.3. Vehicle Entry to Restricted Area.

2.3.1. Government vehicles—including government-contracted rental vehicles—may be operated in the area when required for official business. Drivers or required escorts of vehicles entering ECPs will attest the vehicle has been inspected prior to entry into the restricted area.

2.3.2. Vendors, deliverers, and contractors who must use their vehicle to perform integral parts of their contract/duties require written authorization by the Chief of Security (AF ISR Agency/SO) to enter and operate within the restricted area complex. Escorts of vehicles entering the restricted area will attest the vehicle has been inspected prior to entry into the restricted area.

2.3.3. Privately owned vehicles (POVs) are prohibited from entry to and operation within the area unless authorized by AF ISR Agency/SO.


3.1. Unescorted Entry into the SCIF. Locally assigned personnel with Top Secret clearances and SCI access, entry authority, and an AFISRA Form 325, 325C, 325F, or 325R are authorized unescorted SCIF entry. Likewise, visitors with Top Secret clearances and SCI access, entry authority, and an AFISRA Form 325CT, 325DV, 325T or 325FT are authorized unescorted SCIF entry. NOTE: Entrance to interior rooms requires owner/user concurrence.

3.1.1. Unescorted SCIF entry procedures. Access to the SCIF is controlled through use of proximity access control card readers. Individuals must have a proximity access control badge with access privileges granted. Personal Identification Numbers (PIN) will be required with the proximity badges. Light Emitting Diodes (LED) on the access control reader will alternate blinking red/green continuously indicating the reader is communicating with the annunciator. NOTE: Unit Security Managers provide training to assigned personnel prior to EC issue, document the training via local form (see Attachment 1), and maintain the documentation for program review.
3.1.1.1. Place proximity badge in opposite hand from the one you’ll use to input your PIN. This prevents multiple readings.

3.1.1.2. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

3.1.1.3. Within 5 seconds, input your 4-digit PIN followed by the pound (#) sign. NOTE: If not completed in 5 seconds, pause for a brief moment to allow the system to reset, then redo the entire process beginning with paragraph 3.1.1.2.

3.1.1.4. EXCEPTION: Authorized personnel opening exterior SCIF doors may allow other authorized personnel to enter the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel entering the SCIF must display their EC.

3.1.2. Unescorted SCIF Exit Procedures. When exiting the SCIF, press the panic hardware (door release bar) and push door outward. Exit the SCIF and ensure the door closes securely before walking away. NOTE: Handicapped exit mechanism buttons are for handicapped personnel use only.

3.1.2.1. EXCEPTION: Authorized personnel departing the SCIF may allow other authorized personnel to exit the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel exiting the SCIF must display their EC.

3.1.2.2. If an authorized individual is waiting to enter as you exit the door, ensure they have the proper unescorted entry credential before allowing them entry to the SCIF.

3.2. Escorted Entry into the SCIF. Locally assigned personnel without a Top Secret clearance and SCI access are escorted for the duration of their visit in the SCIF. They are issued AFISRA Form 326, 326C, 326R, or 332 in accordance with paragraph 2.2.1. and 2.2.3. Visitors with a Top Secret clearance with SI access only are issued AFISRA Form 325TY and escorted while in the SCIF. Likewise, visitors without a Top Secret clearance and SCI access are escorted for the duration of their visit in the SCIF. They are issued AFISRA Form 326CT, 326DV, 326T, 332DV, or 332E in accordance with paragraph 2.2.1.4. and 2.2.3.1. NOTE: Entrance to interior rooms requires owner/user concurrence.

3.2.1. Escort Procedures within the SCIF. Personnel with unescorted entry to the restricted area but not the SCIF must report to one of four areas to wait for their escort: Building 2000 first floor foyer, Building 2000 courtyard side foyer, Building 2007 courtyard side foyer and Building 2007 parking lot side. All other personnel requiring escorted entry into the SCIF must report to an ECP or Visitor Control to wait for their escort.

3.2.1.1. Escorted entry applies to individuals with official business to perform within the SCIF and who have not been granted unescorted entry. A trained and certified escort official—all personnel issued AFISRA Form 325-series ECs with photographs except contractors (unless there is an E-1 printed on the contractor’s EC)—must escort these personnel throughout the duration of the visit.

3.2.1.2. Escorts will:

3.2.1.2.1. Be trained and certified annually.
3.2.1.2.2. Outside the SCIF boundary, meet and positively identify individuals requiring escorted entry.

3.2.1.2.3. Print all visitor and escort official point of contact information on the “Escort Required” sign-in log located at Building 2000 first floor foyer, Building 2000 courtyard side foyer, Building 2007 courtyard side foyer and Building 2007 parking lot side. Visitor information includes name, rank/grade, organization or firm, social security number (last six digits only), and citizenship. Escort official information includes purpose of visit, POC name, escort official entry credential number, and time in. **NOTE:** Visitors must exit the SCIF at the same location they entered the SCIF.

3.2.1.2.4. Recite the following visitor briefing to each person under escort. **NOTE 1:** If the visitor received the briefing at the restricted area ECP, skip this step. **NOTE 2:** Group briefings are permitted.

3.2.1.2.4.1. I am (state your name), your escort for this visit. Prior to entering the SCIF, I am required to brief you on security procedures and your responsibilities. While you are in the SCIF, you must be under escort by an authorized individual at all times. You must stay with your escort until you depart the area. You must visibly display your AF ISR Agency entry credential on the front of your outermost garment—above the waist—at all times. If you are stopped or challenged by security forces, you must obey all instructions. Do you have any of the following items with you: personally owned photographic equipment, video equipment, audio recording equipment, computers and associated computer equipment, personal digital assistants, cellular phones, or two-way pagers? These are prohibited items (unless authorized in writing by AF ISR Agency/SO). You may not carry them into the SCIF. I am now required to search all handcarried items, vehicle(s), and equipment you plan to take into the SCIF. Be aware, while you are in the SCIF, your person and all your possessions are subject to inspection. Do you have any questions?

3.2.1.2.5. Maintain positive control and constant surveillance of escorted personnel at all times while in the SCIF. The number of individuals an escort official can escort at one time is based on the known trustworthiness of the visitors and the ability of the escort to have reasonable control of the visitors, but will not exceed 8 visitors.

3.2.1.2.6. Receive authorization from room occupants prior to permitting escorted personnel entry. Sufficient time will be given to ensure occupants have secured classified material. Announce the presence of escorted personnel to all personnel working in the SCI area being visited. **NOTE:** Work centers containing escorted personnel will display AFISRAV A 31-101, *Uncleared Visitor Notice*, a flashing or rotating light, or similar device to indicate the continued presence of escorted personnel who are not indoctrinated for SCI material.

3.3. **Escorted Exit Procedures.** Escort officials will accompany personnel under escort to the same SCIF entry/exit point they initially entered and record “time out” on the “Escort Required” log.

3.3.1. If the person under escort is authorized unescorted entry in the restricted area, the escort’s duty ends at this point.
3.3.2. If the person under escort also requires escort while in the restricted area, the escort official walks the visitor to the ECP they initially entered and complies with procedures IAW paragraph 2.2.4.

4. **Escort Training/Certification.** Individuals who possess appropriate credentials will be formally trained, tested, and certified annually on the duties and responsibilities of an escort official. AF ISR Agency/SO develops training and evaluation materials. Security managers administratively track and document training and certification.

5. **Introduction/Removal of Electronic Equipment, Controlled Items, and Prohibited Items.** Driven by the possibility of technical compromise, electronic equipment shall not be routinely carried in or out of the restricted area. Any equipment introduced or removed from the restricted area is subject to physical inspection at any time. To ensure only authorized items are introduced, entry controllers conduct random and comprehensive inspections of hand-carried items.

5.1. **Personally Owned Electronic Equipment and Media.** The following items may be introduced into the restricted area and SCIF:

   5.1.1. Electronic calculators, electronic spell checkers, and wristwatches without data ports.

   5.1.2. Receive-only pagers.

   5.1.3. Audio equipment with only a “playback” feature (no recording capability), or with the “record” feature disabled or removed. This includes compact disk (CD) players and commercially produced music CDs. **NOTE:** Music CDs are not authorized for use in government computers.

   5.1.4. AM/FM radios.

   5.1.5. All necessary medical equipment.

5.2. **Controlled Items.** The following items may be introduced into the restricted area and SCIF only after written approval by AF ISR Agency/SO or via AFISRA Form 57. **NOTE 1:** Sample Letters of Authorization are posted on the NIPRNet, Global Data Network Drive, “Security” folder, “Sample Request Letters” folder. **NOTE 2:** AFISRA Form 57s are issued IAW paragraph 5.4. **NOTE 3:** Letters of Authorizations can take up to 3 duty days to process.

   5.2.1. Two-way transmitting equipment.

   5.2.2. Audio, visual, and optical recording equipment and associated media.

   5.2.3. Test, measurement, and diagnostic equipment (TMDE).

   5.2.4. Personally-owned and government-owned/leased photographic, video, and audio recording equipment. **NOTE:** This equipment is normally authorized for official award/retirement ceremonies and similar functions in the courtyard area between Building 2000/2007 and the Bernard A. Larger Auditorium.

   5.2.5. Government-owned cellular telephones, computer systems and other portable electronic devices are authorized to be carried within the restricted area with written approval from AF ISR Agency/SO; however they will not be turned on or used within the restricted area.

   5.2.6. Government-owned Portable Digital Assistants.

5.3. **Prohibited Items.** The following items are prohibited in the restricted area and SCIF:
5.3.1. Personally owned computer systems and associated media to include personally (non-commercially) produced music CDs. **NOTE:** Read/write music CDs are prohibited from entry.

5.3.2. Weaponry; i.e., firearms, ammunition, flares, explosives, incendiaries, and highly volatile liquids and gases.

5.4. **AFISRA Form 57, AIS/Media Authorization Pass.** The unit Information Systems Security Manager (ISSM), or security manager issues (and signs) the form to individuals authorized to introduce and remove the following unclassified material into and from the restricted area and SCIF on a recurring basis:

5.4.1. Unclassified removable automated information systems storage media (i.e., zip disks, micro-floppy diskettes, CDs, removable hard drives, and optical disks).

5.4.2. Unclassified videocassettes.

5.4.3. Unclassified test, measurement, and diagnostic equipment (TMDE).

5.4.4. Media must be marked with an SF 710, *Unclassified Label for ADP Media in SCI Facilities*, or locally generated equivalent. Commercial off-the-shelf (clearly identifiable such as by manufacturer’s label) and housed in the sealed factory package (shrink-wrap) requires no label. **NOTE:** Refer to AFI 31-101/AFISRA Supplement 1, *The Air Force Installation Security Program*, for further information on the use and completion of the SF 710.

5.4.5. Present this form to the entry controller prior to introducing or removing applicable items.

5.4.6. Individuals will surrender AFISRA Form 57s to their ISSM, or security manager when no longer needed/authorized (i.e., prior to PCS, PCA, separation, or retirement). The ISSM, or security manager will subsequently surrender the forms to AF ISR Agency/SOC.

6. **Conference Procedures.** Personnel hosting conferences within the restricted area and/or SCIF contact AF ISR Agency/SOP for processing of attendee clearances and EC issue. **NOTE:** ECs issued to conference attendees do not leave the restricted area.

6.1. **Conference POCs will:**

6.1.1. Provide rosters of attendees to include name, rank/grade, and SSAN to AF ISR Agency/SOP NLT 3 duty days prior to event start.

6.1.2. Hand carry verified clearance memorandum to Visitor Control and sign for requisite ECs.

6.1.3. Establish procedures to issue, collect, control, and return ECs.

7. **Intrusion Detection System (IDS).** Certain areas within the SCIF require personnel to access and secure alarms. Areas protected by alarms are accessed when opening for the day and secured when closing for the day.

7.1. **Unit Security Managers will:**

7.1.1. Provide training to personnel prior to requesting area/office alarm access for the individual.

7.1.2. Document individual IDS training via local form (See **Attachment 2**); maintain the documentation for program review.

7.1.4. Update AF ISR Agency Form 314, *Security Alarm Emergency Point of Contact* (POC) and forward to AF ISR Agency/_SO CO (Building 2000/Room 257). AF ISR Agency Form 314 will be updated as needed due to changing personnel requirements or not to exceed every 6 months.

7.2. **Unit Security Alarm Emergency POCs will (when contacted by 37 SFS personnel):**

7.2.1. Respond to the affected alarm point within 60 minutes to conduct an internal inspection of the SCIF.

7.2.2. Attempt to determine the probable cause of the alarm activation.

7.2.3. Reset the alarm prior to departure of the response force.

7.3. **Personnel accessing alarms will:**

7.3.1. Enter the alarmed area and proceed directly to the card reader. **NOTE 1:** LED on the card reader will be “red” if area is alarmed; “green” if the area is accessed. **NOTE 2:** Individuals have 30 seconds from the time they open the door until successful transition of alarms.

7.3.2. Place proximity badge in opposite hand from the one you’ll use to input your PIN. This prevents multiple readings.

7.3.3. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

7.3.4. Input your 4-digit PIN followed by the pound (#) sign.

7.3.5. Listen for three audible beeps (confirms successful transition from secure to access).

7.3.6. After a slight delay, LED will change from red to green, signaling area has been accessed.

7.4. **Personnel securing alarms will:**

7.4.1. Ensure there are no personnel left in the area. Conduct an End of Day Security Check IAW paragraph 8.2. **NOTE 1:** LED on the card reader will be “green” if the area is accessed. **NOTE 2:** Individuals have 30 seconds from the time the LED changes to “red” to exit the area.

7.4.2. Place proximity badge in opposite hand from the one you’ll use to input your PIN. This prevents multiple readings.

7.4.3. Hold (do not wave) your badge directly in front of the reader until you hear two audible beeps.

7.4.4. Input your 4-digit PIN followed by the pound (#) sign.

7.4.5. Listen for three audible beeps (confirms successful transition from access to secure).

7.4.6. After a slight delay, LED will change from green to red, signaling area has been secured.

**NOTE:** Individuals have 30 seconds from the time the LED changes to “red” to exit the area.

8. **General Policy and Procedures.**

8.1. **Nondiscussion Areas.** Nondiscussion areas are clearly defined areas within the SCIF where classified discussions are not authorized due to inadequate sound attenuation. These areas include
hallways, restrooms, and such common areas as the cafeteria, mechanical rooms, entrance foyers, and emergency exit stairwells. **Note:** Classified information will not be introduced into restrooms or the AAFES cafeteria.

8.2. **Access Control/End of Day Security Checks.** Access to individual rooms in Building 2000/2007 where SCI is stored, processed, or discussed will be controlled by assigned personnel, mechanical locks, or card readers that activate door drop pins/magnetic contacts.

8.2.1. Offices with mechanical push-button locks on their doors will ensure locks are engaged or an individual assigned to the room can visually monitor personnel entering or exiting.

8.2.2. Unit Security Managers ensure the lock combination and listing of responsible personnel are annotated on an SF 700 maintained in the IOC.

8.2.3. Accomplish End of Day Security Checks IAW AF ISR Agency Instruction 31-401.

8.3. **Window Protection.** Windows surrounding classified discussion and storage areas will be secured at all times within Building 2000/2007. All windows must be equipped with either blinds and/or curtains. Windows without tinting will have horizontal blinds or curtains closed at all times to prevent outside visual surveillance. Windows with tinting may have curtains/blinds open during daylight hours but closed during hours of darkness or decreased visibility. Horizontal blinds may be angled at 45 degrees as long as visual surveillance is prevented.

8.4. **Photography.** Photography is prohibited in and around the AF ISR Agency restricted area unless approved by AF ISR Agency/CC or AF ISR Agency/SO IAW Lackland AFB Instruction 31-101, *Installation Security Program.*

8.4.1. Photography in buildings 2000/2007 will be for official purposes only. Self-help photographic equipment is available for sign out to authorized personnel from the 690th Intelligence Support Squadron Visual Production Photo Flight (690 ISS/VPM). All self-help photography is to be unclassified. **NOTE:** AF ISR Agency ECs must be removed prior to still or motion photography for operational security (OPSEC) purposes.

8.4.2. Photography of classified material or operations for official classified products requires coordination with AF ISR Agency/SO and the 690 ISS/VPM to preclude unintentional release to unauthorized personnel. **NOTE:** AF ISR Agency ECs must be removed prior to still or motion photography for OPSEC purposes.

8.5. **Freight Elevator Use (Building 2000).** The exterior doors leading to the outside dock area of the freight elevator are alarmed 24/7. The lock on the exterior doors will be removed at 0700 and returned at 1600 Monday-Friday (excluding holidays and official down days). For access during these hours, contact 37 SFS Alarm Monitor (ext. 977-2307) to request access. Do not handle the steel bar that secures the doors prior to contacting the Alarm Monitor (doing so will generate an alarm).

**NOTE:** For access during non-duty hours, report to the 24 hour operations center (IOC), Building 2000, room 219, to receive the combination to the lock. Ensure you contact the Alarm Monitor (ext. 977-2307) prior to handling the steel securing bar and after you have completed use of the door. (Failure to do so will generate an alarm).

8.6. **Entry/Exit Inspections.** Entry/exit inspections serve to deter the introduction of prohibited items/contraband and the removal of classified material. Entry controllers perform random inspections of hand-carried items into and out of the area in conjunction with random antiterrorism measures
between 0600-1800 on normal duty days. At all other times—including weekends, holidays, and 1800–0600 each duty day—entry controllers inspect all hand-carried items brought into and removed from the area.

8.7. **Lost/Destroyed Entry Credentials.** Immediately report the loss or destruction of ECs to Unit Security Managers. Security Managers will accomplish requisite paperwork within 72 hours. **EXCEPTION:** Personnel with discolored or excessively worn badges may bypass Unit Security Managers and proceed directly to Visitor Control for reissue.

**NOTE:** Within AF ISR Agency-managed and AF ISR Agency-administratively supported SCIFs, personnel who forget their badges or have lost their badges; and have yet to be issued a replacement may be issued the appropriate Temporary “T” badge corresponding to their respective clearance level.

8.8. **Entry Credential Turn-in Procedures.** Individuals no longer needing ECs assigned to them—i.e., due to reassignment, separation, or retirement—will report to Building 2000, Room 259, Indoctrination/Debrief Office (AF ISR Agency/SOPI) for debriefing and EC disposition.

8.9. **Prescribed Form:** AFISRA Form 314, Security Alarm Emergency Point of Contact.

8.10. **Adopted Form.** AF Form 847, *Recommendation for Change of Publication.*

JOHN C. KOZIOL, Maj Gen, USAF
Commander
BUILDINGS 2000/2007 SCIF DOOR ACCESS PROCEDURES

All doors will be secured when not in use with the exception of emergency circumstances. If a door must be left open for any length of time due to emergency or other reasons, then it must be controlled in order to prevent unauthorized personnel from gaining access and unauthorized removal of SCI.

**NON-SCIF AREA:** The “Hall of Honor” area inside the glass courtyard doors near the cafeteria and ATM area are **non-SCIF** areas. Red badge personnel and white picture badge holders enter these areas unescorted through the courtyard.

**SCIF ENTRY PROCEDURES:** Access control is granted through use of proximity access control card readers. Individuals must have a proximity access control badge (EC) with access privileges granted. PINs are required for use of the EC.

- Light Emitting Diodes (LED) on the access control readers will alternate blinking red/green continuously *(Indicates the readers are communicating with the annunciator)*
- Place badge in opposite hand from the one inputting your PIN. * (Prevents multiple reading)
- Hold your badge directly in front of the reader *(Do not wave or flash badge)*
- When the reader has successfully read the badge, you’ll hear 2 audible beeps
- After you hear the 2 audible beeps, you have 5 seconds to input your PIN followed by the pound (#) sign * (Do not forget to press the # sign)
- If you don’t complete the process in 5 seconds, you’ll have to pause for a brief moment to allow the system to reset, then attempt the complete process again

**SCIF EXIT PROCEDURES:** Director of Central Intelligence Directive (DCID) 6/9 states, “Personnel entering or leaving an area are required to ensure the entrance or exit point is properly closed.”

- When exiting the SCIF, press the panic hardware (door release bar) and push door outward
- Exit the SCIF, ensuring the door secures before walking away
- If someone is waiting to enter as you exit, ensure they have the proper unescorted entry credential (AF ISR Agency Form 325-series green badge without yellow stripe) before allowing access
- ** (Handicapped buttons are for “handicapped” personnel use only)
ADDITIONAL ENTRY/EXIT PROCEDURES: DCID 6/9 states, “Authorized personnel who permit another individual to enter the area are responsible for confirming the individual’s access.”

Authorized personnel opening exterior SCIF doors may allow other authorized personnel to enter the SCIF behind them, after validating their entry credentials and photo. Visual recognition is not a sufficient validation – all personnel entering the SCIF must display their EC.

ESCORTING PROCEDURES: DCID 6/9 further states, “Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF.” Additionally, DoD 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, states, “A visitor log must be maintained for all visitors.”

- “Escort Required” sign-in logs will be maintained at 2 locations on the first floor of Building 2000 and 2 locations on the first floor of Building 2007
  
  -- Location # 1: Inside the foyer at the bottom of the stairs inside the glass doors at Building 2000
  -- Location # 2: Adjacent to the ATM area
  -- Location # 3: Inside the glass doors of Building 2007 (parking lot side)
  -- Location # 4: Inside the glass doors of Building 2007 (courtyard side)

- Escorting Procedures for Building 2000:
  
  -- Escorted individuals entering the SCIF via the hallway leading to the cafeteria will sign-in at Location # 1
  -- Escorted individuals entering the SCIF via the second/third floors will sign-in at Location # 1
  -- Individuals who enter the non-SCIF area, (see definition above) who require escort into any SCIF area (rear area of 2000, 2nd floor entrance above the ATM, etc.) will sign-in at Location # 2

- Escorting Procedures for Building 2007:
  
  -- Individuals who required escort into Building 2007 (parking lot side) will sign-in at Location # 3
  -- Individuals who require escort into Building 2007 (courtyard side) will sign-in at Location # 4

- Escorted individuals will always be signed-out at the same location they were signed-in
- Phones are located at each location to call for escort officials
- All visitor information must be printed on the sign-in logs to include the “escort official” (point of contact) information
- Due to risks of identity theft, only the last 6 digits of SSNs will be required. ** (This information is mandatory on the sign-in log)
*** Failure to comply with escort requirements will jeopardize our SCIF accreditation

*** Random checks will be conducted to monitor compliance with escort procedures

I acknowledge I have read the above entry/exit instructions and escort procedures. I also understand my individual responsibilities to ensure access is only granted to authorized individuals.

Printed name: ______________________________________________________________

Signature and date: __________________________________________________________

* Hand-carry completed forms to Visitor Control at time of badge issue. Once EC is issued, return the form to Unit Security Manager for filing.
Attachment 2

VINDICATOR ALARM ENTRY/EXIT PROCEDURES

ENTRY (ACCESSING)
- Enter alarmed area and proceed directly to the card reader
- LED on the card reader will be “red” if area is alarmed; “green” if area is accessed
- Hold the proximity card directly in front of the card reader
- Listen for two audible beeps (confirms the card has been read)
- Enter four-digit personal PIN followed by the pound sign (#)
- Listen for three audible beeps (confirms successful transition)
- After a slight delay, LED will change from red to green
- Area has been accessed

NOTE: Individuals have 30 seconds from the time they open the door until successful transition of alarms

EXIT (SECURING)
- Ensure there are no personnel left in the area
- LED on the card reader will be “green” if the area is accessed
- Hold the proximity card directly in front of the card reader
- Listen for two audible beeps (confirms card has been read)
- Enter four-digit personal PIN followed by the pound sign (#)
- Listen for three audible beeps (confirms successful transition)
- After a slight delay, LED will change from green to red
- Area has been secured

NOTE: Individuals have 30 seconds from the time the LED changes to “red” to exit the area.

I acknowledge I have been properly trained by my Unit Security Manager. I understand the entry/exit procedures and my individual responsibilities as described above.

_________________________________________  _______________________
Signature                                    Date

* Unit Security Managers maintain completed forms.