

**BY ORDER OF THE COMMANDER  
480TH INTELLIGENCE SURVEILLANCE  
AND RECONNAISSANCE WING  
(AFISRA)**

**480TH ISR WING INSTRUCTION 31-102**

**10 JUNE 2014**

**Security**



**BUILDING 23 ENTRY PROCEDURES AND  
SECURITY MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 480 ISR WG/SO

Certified by: 480 ISR WG/SO  
(Mr. Larry Wiatrowski)

Pages: 15

---

This publication implements DoD Manual 5105.21 Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*; DoD Manual 5105.21 Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor control, and Technical Security*; DoD Manual 5105.21 Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*; DoD 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*; DoD 5200.01 Volume 2, *DoD Information Security Program: Marking of Classified Information*; DoD 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*; DoD 5200.01 Volume 4, *DoD Information Security Program: Controlled Unclassified Information (CUI)*; Air Force Policy Directive 14-3, *Control, Protection, and Dissemination of Intelligence Information*; AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information*; and AFI 31-401, *Information Security Program*. It prescribes security operating procedures, policies, and responsibilities for Headquarters, 480th Intelligence, Surveillance, and Reconnaissance (ISR) Wing. This instruction applies to all personnel working in or requiring access to Building 23. It requires collecting and maintaining information protected by the Privacy Act of 1974. Send recommendation for changes on AF Form 847, *Recommendation for Change of Publication*, through channels to 480 ISR WG/SO, 34 Elm Street, Joint Base Langley-Eustis, VA 23665-2092. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS)

located at <https://www.my.af.mil/afrims/afrims/afrims/rim.cfm>. Contact supporting records managers as required.

## 1. Duties and Responsibilities:

### 1.1. 480 ISR Wing/Security Office (SO) will:

- 1.1.1. Assign Building 23 personnel appropriate Entry Control Badge(s) (ECB).
- 1.1.2. Ensure all personnel are trained on entry procedures, escort procedures, and proper wear of the ECB.
- 1.1.3. Verify visitor clearances and issue the appropriate ECB.
- 1.1.4. Verify clearances in Joint Personnel Adjudication System (JPAS) or Scattered Castles.
- 1.1.5. Act as the approval authority for any deviation from established procedures.

### 1.2. Building 23 occupants will:

- 1.2.1. Maintain accountability for the proper usage and wear of their permanent ECB.
- 1.2.2. Coordinate with the 480 ISR Wing Special Security Officer (SSO) for procedures when sponsoring a visitor or family member.
- 1.2.3. Adhere to procedures outlined in this instruction.
- 1.2.4. Read the Building 23 Emergency Action Plan.
- 1.2.5. Ensure access to classified information is limited to personnel with a need-to-know, a security clearance commensurate with the material, and a signed a nondisclosure agreement.

### 1.3. Building 23 sponsors will:

- 1.3.1. Coordinate visitor requests through the SO NLT 3 days prior to visit to the 480 ISR Wing/SO Visitor Control Organization box (480ISRWG/[SOVisitControl@langley.af.mil](mailto:SOVisitControl@langley.af.mil)).
- 1.3.2. Meet their visitors in the entry control lobby prior to accessing the building.
- 1.3.3. Maintain accountability for visitor ECBs until they are returned to SO. **NOTE:** Visitor ECBs must not leave the building unless the member is on-site multiple days. **EXCEPTION:** Groups or tours visiting Building 23 and continuing to the 497 ISR Group (GP) can take the ECB out of the building with SSO approval; the conference POC/sponsor is responsible for returning ECBs to SO upon completion of the visit.

## 2. Entry Procedures:

- 2.1. 480 ISR Wing, Building 23, is a controlled area. Hours of operation for the Entry Control Point (ECP) are 0700 to 1600 (as manning permits) Monday through Friday; after duty hours, contact the Wing Operations Center (WOC) at 225-0586. Personnel entering and exiting this facility are tracked either electronically or via the visitor registration log (AF Form 1109). Each individual entering or exiting Building 23 will either sign in/out or utilize the card readers. When requesting entry, individuals are required to present a valid picture

ID, DoD ID number or Social Security Number (SSN) to the SO for identification and clearance verification.

2.2. Building 23 has a single point of entry at the front of the building. All other doors are used for emergency exit only. Door 9 (warehouse/dock) access will be approved on a case-by-case basis and must be approved by the SO.

2.3. Permanent ECBs will be given to military, civilian, contractors, and Air Reserve/Guard members assigned to the 480 ISR Wing, 27 IS and AFOSI. Personnel assigned to the 497 ISR GP requiring swipe-access must get approval from the Chief, Wing Security. (EXCEPTION: 10 IS personnel working full-time in Building 23 do not need SO approval; individuals need to bring their 497 ISR GP badge to Wing SO to be coded).

2.3.1. Personnel with a permanent ECB and a Personal Identification Number (PIN) access the building by swiping the ECB across the badge-reader and entering the PIN on the keypad. If after three attempts, access is not granted and the red light on the ECB reader is lit, the individual must contact the ECP. At no time will an individual without a working permanent ECB be allowed unescorted entry in Building 23.

2.3.2. The ECB will be displayed above the waist with the photograph in plain view at all times.

2.3.3. Personnel who work in Building 23 who forget their ECB will be issued the appropriate "Visitor" badge.

2.3.4. When leaving, personnel must swipe their badge then remove/secure it from sight.

2.4. Federal civilian employees, military personnel, and contractors whose principal place of work is Building 23, are authorized to perform escort duties. Escorts must be thoroughly familiar with their responsibilities (see paragraphs 3 through 3.3.2).

2.5. Personnel will scan their ECB to access authorized areas of Building 23. "Tail-gaiting" or "piggy-backing" (personnel entering without scanning in) is not allowed. **EXCEPTION:** Properly credentialed visitors (reciprocal badge holders and properly escorted individuals) without swipe access may tailgate.

### **3. Escort/ECB Procedures for Visitors:**

3.1. Building occupants must notify the ECP three duty days in advance when visitors are expected. All visitors must have a sponsor assigned to Building 23; sponsors are responsible for their guests while in the facility. All badges will be worn above the waist and displayed with the number and "VISITOR" in plain view at all times. When entering/departing workspaces with individuals who are not indoctrinated or cleared, escorts will carry a flashing red light and loudly announce the presence of a "red" or "blue-badge" to allow personnel time to sanitize the area. These individuals will not be, under any circumstance, left unattended inside the Sensitive Compartmented Information Facility (SCIF). Before leaving the building, escorts will take visitors to the ECP to sign out and turn-in their badge. After duty hours, the badge will be left in the security drop box.

3.2. Green or Yellow ECB. Federal civilian and military personnel who have verified SCI access are issued a green badge. SCI-cleared contractors are issued a yellow badge.

3.3. Blue ECB. Personnel with a verified collateral clearance are issued a blue ECB. These individuals may be allowed to work unescorted in the supply/facility manager's workcenter and the warehouse only. **INDIVIDUALS WILL BE ESCORTED WHEN ENTERING OR DEPARTING THE SCIF.**

3.4. RED ECB. Personnel who do not have a security clearance are issued a red ECB. **THE VISITOR WILL BE ESCORTED AT ALL TIMES WHILE IN BUILDING 23.** The necessity to badge a child will be determined by ECP staff.

3.5. ECBs for Conference Attendees. SCI-cleared personnel who are attending a conference in Building 23 will be issued a green or yellow swipe Visitor ECB. Collateral/uncleared visitors will not have swipe-badge privileges and must remain under constant escort. Visitors will remove and secure the ECB when leaving the facility. At the end of the conference, ECBs will be returned to the sponsor or left in the security drop box. Groups/tours visiting Building 23 and continuing to the 497 ISR GP may take the badge out of the building with approval from the SO; the POC is responsible for returning the badges to 480 ISR WG ECP.

3.5.1. Conference POCs/hosts will coordinate the visit with **SO NLT 3 duty days prior to the event.** Send the attendees' full name, DoD ID Number, organization/company, and duty phone to the Wing Visitor Control Organization box (480ISRWG/[SOVisitControl@langley.af.mil](mailto:SOVisitControl@langley.af.mil)) for clearance verification. POCs will only provide the attendee's SSN if the individual does not have a DoD ID number. Ensure any personally identifiable information (PII) transmitted over NIPRNET is encrypted.

3.5.2. POCs **will be** available to expedite badge-issue on the first day of the conference. They will sign/take responsibility for distributing and collecting all badges; these are controlled items that must be returned to the SO at the end of the conference.

3.6. Personnel not assigned to the 480 ISR WG or 27 IS who require a permanent-access ECB must have a sponsor assigned to Building 23. Requests must be made through the individual's security manager to SO using the *480 ISR WG ECB Request Memorandum (Attachment 2)*. The request must explain the reason and frequency of access. SO will coordinate the request through the wing/vice commander/TD for approval.

3.7. Official deliveries (Base Information and Transfer Center/UPS/FEDEX, etc.) will be scheduled with 480 ISR WG/CCEA at 225-3542 during standard duty hours (Monday through Friday, between 0700 and 1700).

3.8. Lost ECBs. Individuals who lose their ECB must report it to the Security Office within 24 hours of discovery. The member must complete a *Loss of Building 23 Entry Control Badge Memorandum (Attachment 3)*, and turn it in to the Chief, Wing Security, who will hold it for 5 duty days to allow time for recovery. If the ECB is not found after 5 duty days, the letter is processed for investigation. Upon Chief, Wing Security approval, a new ECB will be issued and a copy of the memorandum will be placed in the individual's special security file.

#### 4. After Duty Hours.

4.1. Any Building 23 occupant with swipe access may enter the building for official business with their ECB and PIN.

4.2. Visitors should be limited to normal duty hours. After-hour visitor requests must be coordinated in advance with the SO and 27 IS WOC Chief.

4.3. Unverified emergency responders/maintenance personnel must be escorted at all times while in Building 23. In the event of an emergency, where life, safety, or property are at risk, responders will sign-in on the visitor log after the situation is brought under control.

## 5. Equipment/Material Policy.

5.1. Certain items **will not be brought into the SCIF** because they are potential security/safety hazards; these include firearms, ammunition, and explosive devices. Personally-owned photographic equipment, headphones, video and audio recording devices, e-readers, MP3 players, computers, removable storage media (e.g., flash drives, memory cards, hard drives, personally-owned DVDs), and portable electronic devices (PEDs) are also prohibited.

5.1.1. **Commercially-produced** music CDs must be marked with the owner's name and telephone number; they will only be played on personal CD-players that have been approved by the SO.

5.1.2. **ALL** magnetic media, entering or exiting the SCIF, including items used for official business, must be listed in the media log located in the main hallway. Additionally, **ALL** magnetic media must be registered with the media librarian (225-5620) and deregistered when items are permanently removed from the SCIF or destroyed.

5.1.3. PEDs such as i-Phones or Blackberries will not be brought into the SCIF. If stored in the lobby lockers, phones must be turned off or set on vibrate. This restriction also applies to government-owned equipment.

5.1.4. A *Laptop Authorization Request Memorandum*, (**Attachment 4**), must be submitted and routed through SO (225-8735) and the Building 23 IAO (225-3481) when bringing laptops into the SCIF.

5.2. All personnel are subject to search upon entering/exiting Building 23 and may be asked to present hand-carried items for inspection in accordance with 480 ISR WG Instruction 31-101, *Sensitive Compartmented Information Facilities (SCIF) Entry and Exit Random Inspections*. Inspections are a physical security safeguard to prevent introduction of unauthorized items into the building and to prevent unauthorized removal of government and classified material. Inspections are limited to the articles being carried into/out of the facility and may include purses, briefcases, newspapers, notebooks, magazines, gym bags, etc.

5.3. Photography or videotaping in Building 23 will be for official purposes only. All requests must be approved by the SO using the *Request for Authorization for Videotaping/Still Photography in Building 23* (**Attachment 5**). **NOTE:** Operations security measures require removal of all ECBs prior to photographing/videotaping. Photography of operations for official classified/unclassified products requires prior coordination with SO.

5.4. Building 23 has a 100% shred policy for all paper (including post-its/unofficial mail received from outside or commercial agencies) and magnetic media. Residents will ensure classified/sensitive holdings are kept to a minimum. Unclassified magazines, books, brochures, newspapers, catalogs, etc., may be recycled after removing/shredding the address labels & any preaddressed order forms. (NOTE: Pages with any handwritten notes must be

shredded). Paper shredders are available throughout the building and will be used to destroy unnecessary documents. Memorandums that identify the highest classification level for each machine are posted on/near each shredder. A CD/DVD shredder is located in the security office and media library. Users will notify the media librarian before shredding CD/DVDs so the database can be updated. **Burn bags will not be used in Building 23.**

5.4.1. Hard drives, video/audio tapes, circuit boards, plastic components, and other material that cannot be shredded will be turned in during a scheduled magnetic-media run to Ft Meade MD. Component turn-in will be coordinated with the Building 23 IAO and SO. Do not drop items off at SO for destruction and/or turn-in.

5.4.2. The fourth Thursday in March is designated as the Building 23 Annual Classified Cleanout Day. Each office will review their holdings and destroy all unnecessary items to preclude recognition or reconstruction. Personnel should also use this opportunity to review and destroy unnecessary FOUO/PII material.

## 6. Reciprocity.

6.1. SO accepts all in-scope security clearance or access determinations (without waivers, conditions or deviations) from other AF units and Intelligence-Community agencies.

6.2. The 480 ISR WG has badge reciprocity with Headquarters ACC/A2S, 497 ISR GP and its subordinate units, AFC2IC, Air Force Targeting Center and DGS-X. Picture badges from these organizations are accepted as entry credentials for Building 23; however, individuals must still sign in/out on the visitor log and are authorized to piggy-back/tailgate. Note: 480 ISR WG and 497 ISR GP visitor badges may be used in the other's facility with prior coordination.

## 7. Non-Discussion Areas.

7.1. Classified information will not be discussed in break-rooms, restrooms, and hallways. The SO may designate, as required, other non-discussion areas. Discussing classified information in common areas is a practice dangerous to security and must be reported to SO immediately.

## 8. Building 23 Intrusion Detection System (IDS).

8.1. The building has a 24/7, alarmed IDS on all external doors; monitoring stations are in the ECP and WOC. If an external door is opened, the alarm will sound. It is everyone's responsibility to physically secure the door and *immediately* notify the SO (during duty hours) or WOC (after duty hours). SO or the WOC will contact security forces. If a suspected security breach has occurred, immediately call 633d Security Forces (911) and guard the door until relieved.

8.2. SO personnel will be notified whenever an unannounced alarm or suspected breach occurs. A member of SO, if available, will respond to review security camera footage and assist security forces personnel in their investigation.

## 9. Courier.

9.1. Only individuals who have a DD Form 2501 (Courier Card) or courier authorization letter signed by the SO will remove classified material from Building 23. Couriers will be briefed and are responsible for ensuring material is marked, double-wrapped, and transported

in a locked container. Courier credentials are required when transporting classified material into or out of Building 23. DD Forms 2501 will only be issued to individuals who frequently transport classified material.

9.2. Collateral information, up to SECRET, may be sent through the Building 23 mailroom.

9.3. SCI **or** collateral TOP SECRET material must be mailed via the Defense Courier System (DCS). SO is the POC for DCS shipments.

## 10. Security Management.

10.1. Security is everyone's responsibility. Individuals will ensure all classified material, including folders, binders, working papers, slides and electronic media, is properly marked and protected IAW DoD Manual 5105.21 Vol 1; DoD Manual 5200.01, Vol 2; DoD Manual 5200.01 Vol 3; DoD Manual 5200.01 V4, and the *Intelligence Community Classification and Control Markings Implementation Manual*. Privacy Act (PA) and classified material will be concealed with the appropriate coversheet when not secured or left unattended. Encrypt all unclassified emails containing PII or FOUO information.

10.2. Immediately report all suspected security violations to SO. If necessary, the commander will appoint an inquiry official.

10.3. The SF Form 701, *Activity Security Checklist*, will be used as the end-of-day checklist, at a minimum, in offices with security containers. The containers must be listed on the SF Form 701. Completed forms must be kept for 90 days. If any office routinely closes and secures any additional "inner" vault/secure room at the end of each duty day, the occupant or "owner" of that vault/room will also conduct end of day checks and document them on an SF Form 702 and SF Form 701. For all offices without additional "inner" vaults, secure rooms or containers, the End-of-Day security check conducted by the SO to document securing and alarming of all access points to the facility will suffice. SO will ensure the main entry point's access control system is functioning properly on the SF Form 701.

10.4. The SF Form 700, *Security Container Information*, will be used to record the date the combination is changed, location of the container (or door) and the names, addresses, and home phone numbers of the individuals who will be contacted if the container is found open and unattended. If used, Part II of the SF 700 will be stored in a separate security container that is cleared to the same or higher level.

10.5. The SF Form 702, *Security Container Check Sheet*, will be used to record all security container openings/closings.

10.6. Before using, verify the classification level of copiers and shredders. SO is responsible for ensuring authorization memorandums are posted near each machine.

10.7. At publication, there are no classified faxes in Building 23. Classified digital senders are located in the IAO office and Room 87.

10.8. Individuals **must** report to SO, in writing, any significant changes in personal status which include, but not limited to: name changes; marriage/divorce; cohabitation with or intent to marry a non-US citizen; adverse involvement with law enforcement; DUI/DWI; traffic violations of \$300 or more; credit judgments; bankruptcy filing or repossessions.

10.9. Users must take reasonable steps to minimize unauthorized access to controlled unclassified information (CUI) which includes FOUO material. The individual who possesses/controls the information, not the prospective recipient, determines whether someone has a need for access. CUI must be shielded when not in use or left unattended.

10.10. FOUO material may be sent via first class mail, parcel post, or, for bulk shipments, by fourth class mail. It may also be sent via encrypted email or faxed (the sender is responsible for determining that appropriate protection will be available at the receiving location prior to transmission). Additionally, all unclassified information must be reviewed and approved through standard DoD processes before it is released.

10.11. DoD personnel may be subject to criminal/administration sanctions if they knowingly, willfully or negligently disclose CUI to unauthorized persons.

## **11. Conclusion:**

11.1. The information you have just read is designed to assist you in fulfilling your security responsibilities. It by no means describes the total extent of your obligations to protect classified/CUI material. You are expected to be mindful of the importance of the work being accomplished in Building 23 and the unique sensitivity of its operations.

JEFFREY A. KRUSE, Colonel, USAF  
Commander

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

DoD Manual 5105.21 Volume 1, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, 19 October 2012

DoD Manual 5105.21 Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, 19 October 2012

DoD Manual 5105.21 Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, 19 October 2012

DoD Manual 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, 24 February 2012

DoD Manual 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information*, 24 February 2012

DoD Manual 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

DoD Manual 5200.01 Volume 4, *DoD Information Security Program: Controlled Unclassified Information*, 24 February 2012.

*Intelligence Community Classification and Control Markings Implementation Manual*, 31 May 2011

AFPD 14-3, *Control, Protection, and Dissemination of Intelligence Information*, 1 May 1998

AFM 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information*, 1 May 1999

AFI 31-401, *Information Security Program*, 1 Nov 2005

AFMAN 33-363, *Management of Records*, 24 February 2012

480 ISRWI 31-101, *Sensitive Compartmented Information Facilities (SCIF) Entry and Exit Random Inspections*, 7 February 2011

***Prescribed Forms***

AF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

*Adopted Forms*

DD Form 2501, *Courier Authorization*

*Abbreviations and Acronyms*

**480 ISR WG**—480th Intelligence, Surveillance, and Reconnaissance Wing

**ACC**—Air Combat Command

**AFTC**—Air Force Targeting Center

**CUI**—Controlled Unclassified Information

**DCS**—Defense Courier System

**ECB**—Entry Control Badge

**ECP**—Entry Control Point

**FOUO**—For Official Use Only

**IDS**—Intrusion Detection System

**IS**—Intelligence Squadron

**JPAS**—Joint Personnel Adjudication System

**PA**—Privacy Act

**PED**—Portable Electronic Device

**PII**—Personally Identifiable Information

**PIN**—Personal Identification Number

**SCI**—Sensitive Compartmented Information

**SCIF**—Sensitive Compartmented Information Facility

**SO**—Security Office

**SSO**—Special Security Officer

**WOC**—Wing Operations Center

Attachment 2

480 ISR WG ENTRY CONTROL BADGE (ECB) REQUEST

Figure A2.1. Sample of a 480 ISR WG Entry Control Badge (ECB) Request.

(Letterhead)

Date

MEMORANDUM FOR 480 ISR WG/SO

FROM: (Sponsor's Name, Grade, Office Symbol)

SUBJECT: Building 23 Entry Control Badge (ECB) Request

1. Request approval to issue the following individual a 480 ISR Wing ECB. This individual needs the badge for the following reasons: give detailed rational and how often access to the building is needed.

<u>NAME</u>	<u>RANK</u>	<u>DoD ID</u>	<u>UNIT</u>
-------------	-------------	---------------	-------------

The following information is required if the individual is a contractor

Prime Contract #:

Sub-Contract # (if needed):

Cage Code:

Task Order:

Contract Award Date:

Contract End Date:

2. If the ECB is lost, the member will notify the 480 ISR WG/SSO within 24 hours of discovery. A Loss of Building 23 ECB letter (found in 480 ISRWI 31-102, Attachment 3), will be completed by the member and turned in to SO. The letter will be held in for 5 duty days to allow time for recovery. If the ECB is not recovered after 5 duty days, the letter will be processed for review/investigation. Upon SSO approval, a new ECB will be issued and a copy of the memorandum will be kept in the security office.

3. The member understands that s/he is not allowed to escort other personnel in the building. I will be responsible for the member when s/he is in Building 23.

(Signature Block of Sponsor)

1st Ind: \_\_\_\_\_

The member's request for a Building 23 ECB is approved/disapproved.

NAME, RANK, USAF  
Vice Commander

## Attachment 3

## LOSS OF BUILDING 23 ENTRY CONTROL BADGE (ECB) MEMORANDUM

## Figure A3.1. Sample of a Building 23 lost-ECB memorandum.

(Letterhead)

Date

MEMORANDUM FOR 480 ISR WG/SO

FROM: *(Name, Grade, Office Symbol)*

SUBJECT: Loss of Building 23 Entry Control Badge (ECB)

1. In accordance with AF ISR Agency Instruction 31-101, I am reporting the loss of my ECB.
2. On *(date)*, I discovered the loss of my ECB. The last time I saw it was *(date)* at approximately *(time)* hours. The circumstances surrounding the loss of my ECB are as follows:

*(Briefly describe how you discovered the loss of your card)*

3. I conducted a search of all possible areas and personal belongings with negative results. This is the *(number)* time my ECB has been lost.

(Signature of Member)

1st Ind, 480 ISR WG/SO

TO: 480 ISR WG/SSO

1. The individual has been interviewed concerning the loss of their ECB. An investigation into the facts surrounding the loss has been conducted.
2. Replacement of the ECB **(is/is not)** approved.

(Signature)

480 ISR WG/SO Signature

Attachment 4

LAPTOP AUTHORIZATION REQUEST MEMORANDM

Figure A4.1. Sample request to use a laptop computer in the 480 ISR WG Controlled Area

(Letterhead)

Date

MEMORANDUM FOR 480 ISR WG/SO

FROM: (Rank/Name, Organization/Office Symbol)

SUBJECT: Request Use of Laptop Computer in the 480 ISR WG Controlled Area

\_\_\_\_\_  
Make/Model

\_\_\_\_\_  
Owners Name/Rank

\_\_\_\_\_  
Serial Number

\_\_\_\_\_  
Org/Employer

\_\_\_\_\_  
Building 23 Gov't Sponsor Printed Name

\_\_\_\_\_  
Building 23 Gov't Sponsor Signature

1. Provide details about why the laptop is needed in Building 23 (Who, What, When, Why).
2. In support of the 480 ISR WG mission, my duties require the use of an unclassified/classified (**choose one**) laptop computer in room \_\_\_\_\_ of Building 23, on \_\_\_\_\_ (date).
3. While in the building, I will abide by the following guidelines:
  - a. I will not connect or allow the laptop to connect to any classified network outside the SCIF or any network within the SCIF, nor will I introduce any classified data/media into my electronic device.
  - b. The wireless and recording capabilities will be disabled and verified by the 10 IS/SCOS, 225-5618.
  - c. If it is an unclassified laptop, I understand that my electronic device must remain at least three feet away from any classified system within the controlled area.
  - d. While in the controlled area, I understand that there will not be any modem/network connection or activity.
  - e. I understand that I must maintain physical control and accountability of the laptop at all times within the controlled area.

f. I understand and will comply with all the aforementioned provisions. I accept full responsibility for my actions and the laptop while in the controlled area.

g. I understand that if the laptop becomes compromised or is suspected of compromise, it can be confiscated and or destroyed.

h. This approval letter will always accompany the laptop and a copy will be provided to the 480 ISR WG/SO.

\_\_\_\_\_  
Owner's Signature

1st Ind, 10 IS/SCOS, Request the Use of Laptop Computer in the 480 ISR WG Controlled Area  
Approved/Disapproved.

\_\_\_\_\_  
10 IS/SCOS IAO (Signature)

\_\_\_\_\_  
Date

2nd Ind, Building 23 IAO *(Signature only required if connected to network)*

Approved/Disapproved.

\_\_\_\_\_  
Building 23 IAO

\_\_\_\_\_  
Date

3rd Ind, 480 ISR WG/SO

Approved/Disapproved. This memorandum expires on \_\_\_\_\_

\_\_\_\_\_  
480 ISR WG/SO Signature

\_\_\_\_\_  
Date

Attachment 5

REQUEST FOR AUTHORIZATION FOR VIDEOTAPING/STILL PHOTOGRAPHY IN BUILDING 23

Figure A5.1. Sample request for videotaping/Still Photography in Building 23

(Letterhead)

MEMORANDUM FOR 480 ISR WG/SO

FROM: (Rank/Name, Organization/Office Symbol)

SUBJECT: Request Authorization for Videotaping/Still Photography in Building 23

1. Request approval to videotape/photograph (choose one) inside Building 23 for: \_\_\_\_\_  
\_\_\_\_\_. This event will take place on \_\_\_\_\_ (date) at \_\_\_\_\_ (time).

2. To ensure proper security, I understand and will comply with the following procedures:

a. The room will be properly sanitized prior to video being recorded or photographs taken.

b. Videotaping/photographing will be limited to the unclassified level.

c. The introduction and removal of video equipment or cameras will be annotated on the equipment log located at the SCIF entrance door.

d. All recordings/photographs are subject to review by the 480 ISR WG/SO or designee prior to leaving the SCIF.

3. Point of contact is \_\_\_\_\_ at extension \_\_\_\_\_.

Signature Block of Requestor

1st Ind, 480 ISR WG/SO

MEMORANDUM FOR \_\_\_\_\_ (requestor)

Approved / Disapproved.

480 ISR WG/SO Signature