BY ORDER OF THE COMMANDER
480TH INTELLIGENCE SURVEILANCE
AND RECONNAISSANCE WING (ACC)

480TH INTELLIGENCE,
SURVEILANCE AND
RECONNAISSANCE WING
INSTRUCTION 16-1404

14 FEBRUARY 2023

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** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 480 ISR WG/SO

Certified by: 480 ISR WG/CC
(Col Kayle M. Stevens)

Supersedes: 480ISRWI31-102, 10 June 2014

Pages: 14

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 Manual 5200.01 Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification;* DoD Manual 5200.01 Volume 2, *DoD Information Security Program: Marking of Classified Information;* DoD Manual 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information;* DoD Instruction 5200.48, *DoD Information Security Program: Controlled Unclassified Information (CUI)*; Air Force Policy Directive 14-3, *Control, Protection, and Dissemination of Intelligence Information*; AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*; and AF Manual 16-1404, *Information Security Program*, Volumes 1 through 3. 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. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Record*s, and

disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication;* route AF Forms 847 from the field through the appropriate functional's chain of command. Failure to comply with this publication is punishable as a violation of Article 92, of the UCMJ. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (T-0, T-1, T-2, T-3).

SUMMARY OF CHANGES

This instruction has been revised and must be reviewed.

1. Duties and Responsibilities:

1.1. The 480 ISR Wing Special Security Office (SSO) will:

1.1.1. Issue entry control badges (ECB) to personnel assigned to Building 23

1.1.2. Brief personnel on entry and escort procedures, and proper wear of the ECB.

1.1.3. Verify visitor clearances using authorized means such as the Defense Information System for Security (DISS) (or successor system) or Scattered Castles and issue the appropriate ECB.

1.1.4. Act as the approval authority for any deviation from established procedures.

1.1.5. Issue and file laptop authorization letters.

1.1.6. Submit DISS visit requests (VRs) for 480 ISRW personnel and contractors who are on a wing-owned contract. All other contractors must go through their government lead/owning SSO if a VR is needed prior to travel.

1.2. Building 23 occupants will:

1.2.1. Maintain accountability of their ECB.

1.2.2. Coordinate with the SSO in advance when sponsoring visitors.

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, the appropriate security clearance and a signed nondisclosure agreement. Controlled unclassified information (CUI) will only be discussed/released to those with a need to know.

1.3. Building 23 sponsors will:

1.3.1. Notify visitors to send a DISS VR to SSO480ISRW and confirm receipt in-person or via email to the visitor control mailbox (**480ISRW.SOVisitorControl@us.af.mil**).

1.3.2. Meet visitors at the entry control point (ECP) and maintain accountability for visitor ECBs.

Note: Visitor ECBs will not leave the building except for lunch/breaks; unless the member is on-site multiple days; or the SSO has approved removal.

2. Entry Procedures:

2.1. Building 23 is a controlled area. On duty days, the ECP is open from 0700 to 1600. After duty hours, contact the DCGS Operations Center (DOC) for entry. Personnel entering/leaving the facility are tracked via the ECB or AF Form 1109, *Visitor Registration Log*. When requesting entry, individuals are required to provide a valid government-issued picture ID and/or Social Security Number.

2.2. Building 23 has a single point of entry at the front of the building. All other doors are for emergency use only. The SSO approves all warehouse/dock entry requests.

2.3. Permanent ECBs are issued to federal employees and contractors assigned to Building 23 and AFOSI. The 480 ISRW/DS must approve swipe access requests for personnel assigned to outside organizations.

2.3.1. Personnel with a programmed ECB will access the facility with the badge and PIN.

2.3.2. The ECB will be worn above the waist and must remain visible while in the building. When leaving, personnel will swipe their badge across the reader at the front exit door, then remove or conceal it.

2.3.3. Visitor badges will be issued to personnel who forget their ECB. Individuals who forget or misplace their ECB at least twice a week will be required to have their supervisor meet them at the ECP to sign them in. Individuals who lose their ECB must report it to the security office within 24 hours of discovery. Members will have 5 duty days to recover the badge. If unable to locate the ECB, the member must complete a *Loss of Building 23 Entry Control Badge Memorandum* (Attachment 2) and submit it to the SSO. Upon approval, a new ECB will be issued, and a copy of the memorandum will be filed in the individual's special security file.

2.4. All personnel, including assigned contractors, whose principal place of work is Building 23, are authorized to escort. Escorts must be thoroughly familiar with their responsibilities. Visitors will not escort other visitors, even if they are SCI cleared, without the SSO's approval.

2.5. Tailgating/piggy-backing is not allowed. Personnel will scan their ECB to access rooms with card readers. **Exception:** Reciprocal badge holders and escorted individuals without swipe access may tailgate after signing in at the ECP.

3. Escort/ECB Procedures:

3.1. Building residents who are expecting visitors must notify the ECP 3 duty days in advance. All visitors must have a Building 23 sponsor. Sponsors will sign the AF Form 1109, *Visitor Registration Log*, and ensure guests wear the badge properly. A flashing red light will visually identify non-SCI cleared visitors.

3.2. Escorts will loudly announce the presence of non-SCI-cleared personnel **before** allowing visitors to enter offices. Escorts will not allow individuals with red or blue badges to enter offices first and will ensure the area is sanitized prior to granting entry. Flashlights will be prominently displayed to remind others of uncleared personnel in the area. Before leaving the

building, escorts will take visitors to the ECP to sign out and turn-in ECB. After duty hours, the badge will be left in the security drop box at the front door.

3.3. Green ECBs are issued to SCI-cleared government employees/military. SCI-cleared contractors are issued yellow ECBs.

3.4. Blue ECBs are issued to personnel with a collateral clearance. Individuals **must** be escorted at all times.

Note: The SSO may approve certain blue-badge personnel to go to the bathroom unescorted. Approval is on a case-by-case basis and the SSO is the sole approval authority.

3.5. Red ECBs are issued to uncleared personnel who must remain under escort. ECP staff will determine if children need to be badged.

3.6. Conferences: Conference attendees will be issued the appropriate ECB. If the badge stock is insufficient, ECP staff will issue laminated conference badges. Hosts will ensure an escort is assigned to non-SCI cleared attendees. The host will brief attendees on the requirement to remove and secure ECBs when leaving the building for breaks/lunch.

3.6.1. Hosts will coordinate the visit with the SSO NLT 3 duty days prior to the event. Visit requests must be sent via DISS to SSO480ISRW.

3.6.2. If there are more than 10 attendees, the host will be available to oversee badge distribution on the first day and collection on the last day.

3.6.3. Conference hosts must coordinate, in advance, follow-on visits to the 497 ISRG. Groups visiting Building 23 and continuing to the 497 ISR GP may take the badge out of the building with the SSO's approval—the host is responsible for returning the badges to ECP. Any other visits to on-base units require a DISS VR from the member's SSO/security manager.

3.7. The 480 ISRW Commander, Vice Commander or Technical Director must approve ECB requests for individuals not permanently assigned to Building 23.

3.8. Official deliveries will be scheduled through 480 ISRW/CCEA during duty hours.

4. After Duty Hours:

4.1. After duty hours, the DOC monitors the intrusion detection system (IDS) and responds to alarms.

4.2. Any building resident with swipe access may enter for official business with their ECB.

4.3. Visits should be limited to normal duty hours. After-hour visitor requests must be coordinated in advance with the SSO and DOC Crew Commander.

4.4. Maintenance personnel must be escorted at all times. If it is safe, emergency responders will be escorted by the SSO, facility manager or senior person in charge. If necessary, SSO or senior person in charge will provide inadvertent disclosure agreements to responders once the emergency has passed.

5. Equipment/Material:

5.1. Prohibited items include, but are not limited to, firearms, ammunition, knives with blades longer than 3 1/2-inches, sabers/swords, Mace/pepper spray and explosives.

5.2. Other prohibited items include, but are not limited to, telephones, personally-owned headphones with embedded microphone or noise-cancelling technology; e-readers; tablets; virtual reality goggles/headsets, devices, including watches marketed as "smart", and/or camera glasses; MP3 players; personally-owned computers, removable storage media (e.g., flash drives, memory cards, hard drives, personally-owned DVDs) and most other portable electronic devices (PEDs). Bluetooth-enabled devices such as helmets, calculators, language translators, diagnostic equipment, etc., are also prohibited.

5.3. Personnel who must wear/use electronic medical devices must notify the SSO immediately.

5.4. Client Systems will sign the laptop authorization letter to verify that cellular, Wi-Fi, recording capability and infrared (IR) ports have been disabled before the SSO will approve any electronic equipment to enter the facility. If the equipment will be connected to any network, the memorandum must also be signed by 480 ISRW/DA prior to the SSO's approval.

5.5. Fitness devices and breast pumps with Bluetooth technology are allowed as long as they do not have audio, video, photographic or other wireless capability. Remotes/pointers and other IR devices with no text, audio or recording capability are allowed.

5.5.1. The SSO must approve, in writing, the use of personal CD-players. Commercially-produced music CDs must be marked with the owner's name and telephone number and will not be played on government-owned equipment. The items will be added to the equipment and media logs located in the ECP.

5.5.2. Media/equipment entering or leaving the facility, including items used for official business, will be added to the media/equipment log. Media must also be registered with the media custodian. The custodian must be notified when items are permanently removed from the facility or destroyed.

5.5.3. Telephones stored in the lobby lockers must be turned off or set on vibrate. If a PED is unintentionally brought into the facility, the user agrees that the Government, or its representative, may seize it for physical and forensic examination. Use of lockers constitutes consent to examination, inspection and search of its contents by authorized personnel. Claims for loss for damage to personal items stored in the lockers must be filed through applicable AF claims channels.

5.5.4. All personnel are subject to search upon entering/exiting Building 23. Individuals may be asked to present hand-carried items for inspection IAW AFMAN 14-403, Se*nsitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*. Inspections are a physical security safeguard to prevent introduction of unauthorized items into the building and to prevent unauthorized removal of sensitive 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.

5.5.5. Photography/videotaping in Building 23 will be for official purposes only. Requests must be approved by the SSO using the *Request for Authorization for Videotaping/ Still Photography in Building 23* (Attachment 3). Badges will be removed prior to photographing/videotaping. Photography of operations requires prior coordination with the SSO.

5.5.6. Building 23 has a 100% shred-as-you-go policy for all paper, including post-its/mail 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, pre-addressed order forms and any pages with handwritten notes. Paper shredders are available throughout the building and will be used to destroy unneeded 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, DOC and media library. Users will notify the media librarian before shredding CD/DVDs so the database can be updated. **Burn bags are not authorized in Building 23**.

5.5.7. 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 an approved destruction facility. Component turn-in will be coordinated with the 480 ISRW/DA and SSO. Do not drop items off at security for destruction and/or turn-in.

5.5.8. The fourth Wednesday in March is the designated Building 23 Annual Classified Cleanout Day. Each building resident 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 CUI/Personally Identifiable Information (PII).

6. Reciprocity:

6.1. The SSO 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 wing has badge reciprocity with ACC/A2S/A5/8/9, 363 ISRW, 497 ISRG, Air Force Targeting Center and DGS-X. Picture badges from these organizations are accepted as entry credentials. Individuals without swipe access must sign in/out at the ECP.

7. Non-Discussion Areas: Classified information will not be discussed in break-rooms, restrooms, or hallways. The SSO 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 the SSO.

8. Building 23 IDS:

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

8.2. Notify the SSO whenever an unannounced alarm or suspected breach occurs. The SSO will, if available, review security camera footage and assist security forces.

9. Courier:

9.1. The transportation requirements of DAFMAN 16-1404 Volume 3, *Protection of Classified Information*, will be met before classified material is removed from Building 23. Only individuals who have an SSO-issued courier letter or DD Form 2501, *Courier Authorization*, are authorized to courier. The SSO will brief personnel prior to issuing courier

credentials. Courier cards will only be issued to those who frequently transport classified material.

9.2. Couriers are responsible for marking, addressing and double-wrapping material. Inner and outer wrappers will be secured with reinforced brown "Kraft" tape in order to detect tampering and prevent accidental exposure during transit. Items that are too large or bulky for a briefcase/pouch will be double-wrapped with an opaque cover such as black trash bags. Locked briefcases and zippered pouches may be used as the outer wrapper. DoD contractors may courier only if authorized on the DD Form 254, *DoD Contract Security Classification Specification*.

9.3. Use the AF Form 310, *Document Receipt and Destruction Certificate*, when mailing or when classified information is hand-carried and not returned.

9.4. Collateral confidential and secret information will be mailed through 480 ISRW/CCEA. The Defense Courier Service (DCS) will be used to ship SCI and collateral Top Secret material. The SSO is the DCS liaison. Action officers (AO) will prepare the AF 310 and double wrap the package. The AO will contact the recipient if the AF Form 310 is not received within 15 duty days for CONUS shipments or 30 duty days OCONUS.

10. Security Management and Information Protection:

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.* Use the appropriate Privacy Act, CUI or classified coversheet to conceal unattended material. Encrypt unclassified emails containing PII/CUI.

10.2. Immediately report all suspected security violations/data spills to the 480 ISRW/DA and SSO in-person or via SIPRNET/JWICS/secure VoIP. Do not make notifications via NIPRNET or unclassified telephone. Take custody and safeguard any unsecured classified material.

10.3. If the suspected violation involves collateral information, the commander or section commander will appoint an inquiry official (IO) in writing within 2 duty days from discovery. The IO must be equal to or higher in rank/grade than the person suspected of causing the incident. IOs must be an officer, senior noncommissioned officer or GG-9 or above. The SSO will contact the 633 ABW Information Protection (IP) Office for a case number. The IP Office will brief the IO on their duties. IOs will submit their report to the SSO on SIPRNET within 10 duty days from appointment. The SSO will review the report prior to submitting it to the IP Office. The report must be unclassified and marked CUI or FOUO. If an extension is required, the commander must approve it in writing before the suspense date. The SSO will immediately notify the 633 ABW/IP of any suspense changes.

10.4. The senior intelligence officer will appoint an inquiry official in writing for violations involving SCI. The SSO will notify the MAJCOM SSO for a case number within 24 hours or the next duty day after discovery. Inquiries involving SCI must be completed on JWICS within 30 calendar days and will appropriately classified. If the inquiry cannot be completed by the suspense date, the SSO must be notified immediately.

10.5. For incidents involving the discovery of cellular/radio frequency/IR in the facility, the commander, in consultation with the 633 ABW/IP and/or servicing legal office, determines the disposition of the device. Government devices may be confiscated to determine if it is contaminated with classified information. If a personal device is contaminated with classified information and the individual refuses to surrender it, the commander will consult with the legal office on how to resolve the issue. An AF Form 1297, *Temporary Issue Receipt*, or similar document, will be used if a government or personal device is confiscated.

10.6. 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, *Security Container Check Sheet*, and SF Form 701. For offices without additional "inner" vaults, secure rooms or containers, the end-of-day security check conducted by the SSO to document securing and alarming the facility access points, will suffice.

10.7. Document safe/lock inspections on the OF 89, *Maintenance Record for Security Type Equipment*. The person responsible for the safe/lock will inspect the container/device initially and every 5 years thereafter using the checklist in AFMAN 16-1404, I*nformation Security Program Protection of Classified Information*, Volume 3, Enclosure 3, Appendix 2. The 2-letter director will maintain a current list of names of people who have the safe/lock combination. Reset combinations to 50-25-50 when no longer used to store classified information.

10.8. 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. Part II of the SF 700 will be stored in a separate security container that is cleared to the same or higher level.

10.9. Use the SF Form 702, *Security Container Check Sheet*, to record opening and closing security containers.

10.10. Before using, verify the classification level of copiers and shredders. The SSO will ensure authorization memorandums are posted near each machine.

10.11. At the time of publication, there are no classified faxes in Building 23. Check with the 480 ISRW/DA for the location of classified scanners.

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

10.13. CUI may be sent via first class mail, parcel post, or, for bulk shipments, 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.

All unclassified information must be reviewed and approved through standard DoD processes before it is released.

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

11. Contractors:

11.1. For on-site, permanent contractors, the government representative will provide a copy of the DD Form 254, *DoD Contract Security Classification Specification*, and Statement of Work/Performance Work Statement to the SSO. The security office must be notified immediately when contracts are terminated or when the period of performance changes.

11.2. The SSO will screen all documentation pertaining to security requirements for prime and subcontractors. The facility security officer (FSO) will provide a current list of personnel supporting the contract.

12. Indoctrination/Debriefing:

12.1. When possible, eligible personnel will be scheduled for indoctrination within 2 duty days of arrival. Contractors who are not on a wing-owned contract will be indoctrinated upon receipt of an indoctrination request from the owning SSO.

12.2. The SSO will read eligible personnel into all authorized SCI caveats and NATO-Secret (NATO-S). Individuals with a final secret clearance and those cleared for interim SCI will be read into NATO-S. The SSO will update accesses DISS (or successor system) within 1 duty day.

12.3. Government personnel who are transferring to another AF unit and need to maintain SCI access, must contact the gaining SSO to determine if they will accept a transfer-in-status (TIS). If the gaining SSO will accept a TIS, provide the DISS Security Management Office code and SSO point of contact to wing security.

12.4. If the gaining until does not accept a TIS, personnel must make an appointment, at least 3 duty days prior to departure, to be debriefed.

12.5. Military personnel must coordinate with 480 ISRW/CCEA to make an appointment for out-processing. After debriefing, the SSO will confiscate the ECB and escort the member to the commander's support staff.

12.6. Federal civilians must out-process through 480 ISRW/MS prior to debriefing. Contract/government-leads will contact the SSO to set up debrief appointments for departing contractors. Security will confiscate the ECB and, if necessary, any other government-issued access credentials.

12.7. Personnel must clear their desk and remove their belongings prior to debriefing.

13. Periodic Reinvestigations (PRs) and Reporting Requirements:

13.1. Individuals are required to obtain and maintain a Top Secret clearance with SCI eligibility. PRs will be submitted IAW federal guidelines, currently every 6 years from the anniversary of the last investigation's close date. PRs will be submitted to the 633 ABW/IP no earlier than 3 months from the anniversary month. Personnel must have 12 months remaining in service or employment in order to have a PR initiated. Commanders will grant

continued access for government employees with less than 12 months retainability. Contractor PRs are submitted through the company FSO.

13.2. Report to the SSO, in writing, any significant changes in personal status which include but it not limited to, foreclosure/short sale; arrests; imposition of a restraining/no-contact order; name change; marriage; divorce; cohabitation or intent to marry a non-US citizen; DUI/DWI; traffic violation fines/penalties of $300 or more; credit judgments; bankruptcies or repossessions.

14. Training:

14.1. The SSO will provide an initial security orientation to newly assigned personnel. Individuals assigned to the 480 IRW, including contractors, must complete all required training when tasked.

14.2. Newly assigned personnel will contact accounts management to ensure they are added to the "480 ISR WG Bldg 23" distribution list.

15. Foreign Travel:

15.1. Individuals planning **any** foreign travel must report to the SSO NLT 30 days prior to departure for foreign travel and risk-of-capture briefings. NAVAIR contractors must go through NAVAIR SSO channels for their foreign travel briefing.

16. Accountable Material:

16.1. NATO-S and collateral Top Secret material have specific control, dissemination, and destruction protocols. The SSO is the Top Secret control officer and NATO sub-registry manager. Individuals who need to maintain any accountable items must notify the SSO immediately.

17. Conclusion:

17.1. The information in this instruction will assist you in fulfilling your security responsibilities to protect classified/CUI material and the sensitivity of the 480 ISRW's operations.

KAYLE M. STEVENS, 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 Instruction, 5200.48 Volume 4, *DoD Information Security Program: Controlled Unclassified Information,* 6 March 2020

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

AFM 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* 23 December 2016

AFMAN 16-1404, Volume 1, *Information Security Program: Overview, Classification, and Declassification*, 11 January 2021

AFMAN 16-1404, Volume 2, *Marking of Information,* 7 January 2021

AFMAN 16-1404, Volume 3, *Information Security Program Protection of Classified Information,* 23 December 2020

AFMAN 33-363, *Management of Records,* 28 July 2021

Prescribed Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 310, *Document Receipt and Destruction Certificate*

DD Form 2501, *Courier Authorization*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

OF 89, *Maintenance Record for Security Type Equipment*

Adopted Forms

AF Form 1109, *Visitor Register Log*

AF Form 1297, *Temporary Issue Receipt*

Abbreviations and Acronyms

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

ACC—Air Combat Command

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

JWICS—Joint Worldwide Intelligence Communication 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

SIPRNET—Secure Internet Protocol Router Network

SSO—Special Security Officer

TIS—Transfer in Status

Attachment 2

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

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 480 ISRWI 16-1404, I am reporting the loss of my ECB.

2. On (***date***), I discovered my ECB was missing. The last time I saw it was (***date***) at approximately (***time***). The circumstances surrounding the loss are as follows:

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

1. I conducted a search of all possible areas and personal belongings and am unable to locate it. This is the (***number***) time my ECB has been lost.

(Signature of Member)

1st Ind, 480 ISR WG/SO
Replacement of the ECB (**is/is not)** approved.

MARK A. YOUNG, DAFC
Director, Security

Attachment 3

SAMPLE REQUEST FOR AUTHORIZATION FOR VIDEOTAPING/STILL PHOTOGRAPHY IN BUILDING 23

MEMORANDUM FOR 480 ISR WG/SO

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

SUBJECT: Request Authorization for Videotaping/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 sanitized prior to video being recorded or photographs taken.

b. Videotaping/photographing will be at the unclassified level.

c. The introduction/removal of equipment will be annotated on the equipment log.

d. All recordings/images are subject to review by the SSO prior to leaving the facility.

3. Point of contact is_____at extension_____.

Signature Block of Requestor

1st Ind, 480 ISR WG/SO

MEMORANDUM FOR_____(requestor)

Approved / Disapproved.

MARK A. YOUNG
Director, Security