BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-203, VOLUME 1

31 OCTOBER 2005

Communications and Information

EMISSION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCA/EVPI (Mr. Cyril Prikazsky) Certified by: SAF/XCIA (Mr. David G. Ferguson)
Supersedes AFI 33-203, 26 September 2002 Pages: 35
Distribution: F

This Air Force instruction (AFI) implements the emission security (EMSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and establishes Air Force information assurance (IA) countermeasures and EMSEC requirements for IA. It interfaces with AFI 33-201, Volume 1, *(FOUO) Communications Security (COMSEC)*; AFI 33-202, Volume 1, *Network and Computer Security*; and AFI 33-204, *Information Assurance Awareness Program* (will become AFI 33-204, *Information Assurance Education, Training, and Awareness Program*). This instruction applies to all Air Force military, civilians, and contractor personnel under contract by the Department of Defense (DOD) that participate in the emission security program. This instruction applies to the Air National Guard (ANG). We encourage the use of extracts from this instruction. Additional security instructions and manuals are listed on the Air Force website at **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate channels, to HQ Air Force Communications Agency (HQ AFCA/EVPI AF-CTTA), 203 W. Losey Street, Room 2000, Scott AFB IL 62225-5222, or the EMSEC organizational E-mail box at **afca.ctta.emsec@scott.af.mil**. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force (AF) IMT 847, **Recommendation for Change of Publication**. Send an information copy to Secretary of the Air Force (SAF/XCIA), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363), and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds/index.cfm**. See **Attachment 1** for a glossary of references and supporting information used in this instruction.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2005-01 (**Attachment 5**). Upon incorporation of IC 2005-1, the number of this publication changes from AFI 33-203, *Emission Security* to AFI 33-203, Vol-

ume 1, *Emission Security*, to comply with Air Staff's direction to align all EMSEC publications to be under the AFI 33-203 umbrella. It updates office symbols, changes some forms to IMTs, and updates publications throughout the entire instruction. A bar (|) indicates a revision from the previous edition.

1. Introduction . A major goal of IA is to assure the availability, integrity, and confidentiality of information and information systems. To this end, the IA disciplines of communications security (COMSEC), computer security (COMPUSEC), and EMSEC are, of necessity, interdependent. EMSEC mostly supports the "confidentiality" requirement.

1.1. The objective of EMSEC is to deny access to classified and, in some instances, unclassified information and contain compromising emanations within an inspectable space. Instances of when you must consider unclassified information are addressed in AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)* (will become AFI 33-203, Volume 2 *(S), Emission Security Assessments (U)*). The term "classified information," as used in this instruction, includes those instances. This is accomplished by identifying requirements from the broader view of IA and providing the appropriate protection at the least possible cost. Key to this is a partnership between the IA office and the user.

1.1.1. The user identifies the information systems that will process classified information; the volume, relative sensitivity, and perishability of the information; the physical control measures in effect around the area that will process classified information; and applies identified IA and EMSEC countermeasures.

1.1.2. The wing IA office identifies required IA countermeasures; assesses the need for EMSEC as part of IA; determines the required EMSEC countermeasures; advises commanders of vulnerabilities, threats, and risks; and recommends a practical course of action.

1.2. Committee on National Security Systems (CNSS) used risk management principles to develop the minimum EMSEC requirements identified in this AFI. Since the risk has been accepted at the national level, no further risk for EMSEC can be accepted.

2. Responsibilities and Authority . This instruction establishes the following responsibilities and authorities:

2.1. HQ USAF/XICIA. Responsible for EMSEC policy according to AFPD 33-2. Establishes Air Force EMSEC policy and doctrine, and coordinates with the other military departments and government agencies to eliminate duplication and to exchange technical data. Appoints Air Force Certified TEMPEST Technical Authorities (CTTA).

2.2. HQ USAF/ILE. The Office of the Air Force Civil Engineer is the Air Force focal point for design and construction of facilities containing radio frequency interference (RFI) and electromagnetic interference (EMI) shielding.

2.2.1. Headquarters Air Force Civil Engineer Support Agency (HQ AFCESA/CESM). Responsible for guidance, information, standards, and requirements for design and construction of facilities containing RFI and EMI shielding.

2.3. Headquarters Air Education and Training Command (HQ AETC). In addition to the responsibilities in paragraph **2.8.**, HQ AETC will:

2.3.1. Train or provide training to installers, operators, and maintenance technicians of information systems who process classified information.

2.3.2. Conduct EMSEC training according to AFI 36-2201, *Developing, Managing, and Conducting Training*.

2.3.3. Work with HQ AFCA/EVPI AF-CTTA to make sure EMSEC portions of curriculums are current and meet Air Force needs.

2.4. Headquarters Air Force Materiel Command (HQ AFMC) (includes all program management offices [PMO] located at the Electronic Systems Center Central Design Activity, the Materiel Systems Group, and the Standard Systems Group). In addition to the responsibilities in paragraph **2.8.**, HQ AFMC:

2.4.1. Makes sure EMSEC-related configuration control information is available to the operations, maintenance, and logistics support organizations to maintain the integrity of countermeasures during an information system's life cycle.

2.4.2. Issues time compliance technical orders and modification kits for equipment and information systems processing classified information that are under its inventory management control and scheduled for modification.

2.4.3. Establishes configuration control procedures to ensure the continuity and integrity of countermeasures for equipment and information systems that process classified information under its inventory management.

2.4.4. Makes sure technical analyses, cost estimates, and modification proposals for information systems that process classified information consider TEMPEST design and installation requirements.

2.4.5. Conducts a studies and analysis program that will result in research, development, test, and evaluation of TEMPEST test equipment and techniques. Coordinates TEMPEST information exchange with the Air Force Information Warfare Center (AFIWC/346 TS/TSF), 250 Hall Boulevard, Suite 150, San Antonio TX 78243-7063.

2.4.6. Uses the host IA offices at its engineering and development centers to make EMSEC assessments and countermeasures reviews for its program managers.

2.4.7. Installs equipment and information systems according to EMSEC standards.

2.4.8. Makes sure installation standards retain or enhance EMSEC integrity.

2.4.9. Coordinates exchange of engineering and installation EMSEC information with HQ AFCA/EVPI AF-CTTA.

2.4.10. Performs shielding effectiveness testing when requested.

2.4.11. Provides, when requested, cost estimates for the installation of required countermeasures. Estimates do not include costs based on good engineering practices as EMSEC countermeasures costs. Cost estimates reflect only the delta increase of countermeasure costs.

2.5. HQ AFCA:

2.5.1. Advises HQ AETC on EMSEC curriculum.

2.5.2. Reviews, approves, or disapproves the installation plans that have EMSEC requirements when the installation is contracted.

2.5.3. Provides Air Force organizations disposition instructions for TEMPEST-certified and formerly TEMPEST-certified equipment.

2.5.4. Maintains files of EMSEC countermeasures reviews and waivers.

2.5.5. Reviews national TEMPEST publications and identifies those required for issuance to Air Force activities. Publications with special applications at outside the continental United States bases will be identified. Post a list of required EMSEC program publications on the HQ AFCA IA home page.

2.5.6. Is assigned CTTA responsibility (see paragraph **2.6.**).

2.6. CTTA:

2.6.1. Validates all EMSEC countermeasures reviews.

2.6.2. Issues Emission Security Information Messages (ESIM)s.

2.6.3. Distributes guidance on the domestic and foreign technical threat environment as provided by the CNSS.

2.6.4. Tasks all Air Force EMSEC testing.

2.6.5. Provides Air Force EMSEC requirements and guidance for Air Force information systems.

2.6.6. Represents the Air Force at DoD and national-level TEMPEST forums.

2.7. Headquarters Air Intelligence Agency (HQ AIA). Through AFIWC:

2.7.1. Provides information systems, communications systems, and cryptographic equipment testing and a quick reaction capability to support emergency testing of facilities.

2.7.2. Provides a capability to test high value Air Force systems such as special air mission aircraft and strategic systems (e.g., F-117, B-2, or special access required programs).

2.7.3. Provides a testing and evaluation capability for Air Force information systems in a laboratory environment for zoning and profiling.

2.7.4. Secures a fee-for-service contracting vehicle for routine and standard EMSEC testing support.

2.7.5. Manages the Air Force EMSEC testing program to include contract monitoring and oversight duties.

2.7.6. Provides technical oversight of all contracted Air Force EMSEC tests.

2.7.7. Interacts with the U.S. Government TEMPEST technical community.

2.7.8. Serves as the Air Force technical consultant for emerging EMSEC issues.

2.8. Major Commands (MAJCOM) (includes those field operating agencies [FOA] and direct reporting units [DRU] who have established IA offices [see paragraph **2.8.1.**]):

2.8.1. Establish EMSEC in the MAJCOM IA office.

2.8.2. Include EMSEC requirements identified by the MAJCOM IA office in requests for proposal, specifications, statements of work, operational requirements documents (ORD), program management directives (PMD), and contracts when planning and programming for a procurement requirement for information systems (includes facilities and individual pieces of equipment) that will process classified information. This includes information systems under development and information systems embedded in weapons systems. Review mission need statements (MNS) and equipment specifications for EMSEC considerations and criteria.

2.8.3. Include EMSEC requirements when preparing the COMSEC appendix to the communications annex of operations plans according to AFMAN 10-401, Volume 1, *Operation Plan and Concept Plan Development and Implementation*.

2.8.4. Implement and maintain required countermeasures for information systems that process classified information.

2.8.5. Notify wing and regional civil engineers of any unique construction needed to support programs that process classified information.

2.9. MAJCOM IA Office:

2.9.1. The office of primary record for MAJCOM EMSEC requirements.

2.9.2. Makes sure the individual responsible for EMSEC in the IA office receives EMSEC training.

2.9.3. Provides EMSEC guidance and assistance to the command staff and subordinate IA offices. Include those Air National Guard (ANG) and United States Air Force Reserve (USAFR) units gained by the MAJCOM upon activation.

2.9.4. Implements ESIMs.

2.9.5. Assists wing IA offices by making EMSEC assessments, countermeasures reviews, and EMSEC inspections when requested. Include those ANG and USAFR units gained by the MAJCOM upon activation.

2.9.6. Ensures inspection of all MAJCOM facilities that have EMSEC requirements (see paragraph **8.**).

2.9.7. Reviews and approves EMSEC requirements for contractor facilities for MAJCOM contracts.

2.9.8. Coordinates with the MAJCOM formal training office to establish an EMSEC training priority system so units with the greatest need for formal EMSEC training receive the highest priority.

2.9.9. Assists and provides guidance to the MAJCOM civil engineer for correction of real property EMSEC deficiencies.

2.9.10. Reviews MAJCOM programming and requirements documents that call for the processing of classified information.

2.9.11. For projects that involve more than one wing within the MAJCOM or for MAJCOM programs:

2.9.11.1. Reviews all project support agreements (PSA), project packages, and installation plans, including revisions, for facilities that process classified information.

2.9.11.2. Coordinates with affected wings for the EMSEC assessments and countermeasures reviews.

2.9.11.3. Advises command program managers of required EMSEC countermeasures.

2.10. Host Air Force Wing:

2.10.1. Establish EMSEC in the host wing IA office. The IA office addresses all EMSEC requirements on the base, including those of tenant units (i.e., FOAs, DRUs, and other MAJCOM units), unless there are other formal agreements.

2.10.1.1. Provides IA support for non-Air Force units upon request.

2.10.1.2. Provides IA support for geographically separated units. Any unit not on an Air Force installation may request support from the nearest IA office.

2.10.2. Ensures an IA representative attends planning meetings for new equipment procurement, installation, or reconfiguration of existing facilities that process classified information.

2.10.3. Assist the wing IA office to determine EMSEC requirements and, when required, cost estimates of required countermeasures for new facility construction or upgrade projects.

2.11. Wing IA Office:

2.11.1. Manages wing EMSEC requirements.

2.11.2. Makes EMSEC assessments of all information systems that process classified information on the base, including tenant and geographically separated organizations, unless there are other formal agreements (see paragraph **4.**).

2.11.3. Makes EMSEC countermeasures reviews when required (see paragraph **5.**).

2.11.4. Makes EMSEC inspections to determine compliance with EMSEC requirements. (see paragraph **8.**).

2.11.5. Certifies the information system as meeting EMSEC requirements (see paragraph **9.**).

2.11.6. Makes reassessments as required (see paragraph **11.**).

2.11.7. Implements ESIMs.

2.11.8. Maintains a file of all current EMSEC assessments and countermeasures reviews.

2.11.9. Forwards a copy of all EMSEC countermeasures reviews according to AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews* (will become AFI 33-203, Volume 3, *Emission Security Countermeasures Reviews*).

2.11.10. Ensures the individuals responsible for EMSEC in the wing IA office receives EMSEC training.

2.11.11. Advises commanders, managers, supervisors, and users of countermeasures required to adequately protect classified information (the countermeasures review) and what deficiencies exist for their information systems (the EMSEC inspection).

2.11.12. Maintains a file of all active temporary and permanent waivers.

2.11.13. Ensures current required Air Force EMSEC guidance and information are given wide dissemination.

2.11.14. Provides 38th Engineering Installation Group and systems networking personnel with countermeasures requirements for information systems before engineering and installation begins.

2.11.15. Assists the wing civil engineer in planning new facilities, or reconfiguring existing facilities, that process classified information. Advises the wing civil engineer of any countermeasures requirements for new construction or upgrade projects.

2.11.16. Reviews and approves required countermeasures for contractor facilities supporting wing contracts.

2.11.17. Helps the contracting officer obtain standards necessary for contractual compliance with EMSEC requirements.

2.11.18. Reviews all PSAs, project packages, and installation plans, including revisions, for facilities that will process classified information, to include applicable EMSEC requirements.

2.11.19. Assists users with the technical aspects of applying countermeasures.

2.12. Program Managers are:

2.12.1. Responsible for early coordination with MAJCOM IA offices, Special Category (SPECAT) EMSEC personnel, and wing IA offices to:

2.12.1.1. Make sure EMSEC requirements are in MNSs, ORDs, PMDs, etc.

2.12.1.2. Establish EMSEC requirements at the locations identified for information systems installations.

2.13. Air Force Information Systems Users:

2.13.1. Contact the wing IA office for assistance when the need to process classified information arises.

2.13.2. Request the wing IA office make an EMSEC assessment to identify the need for EMSEC at the earliest date possible.

2.13.3. Implement required countermeasures.

2.13.4. Request the wing IA office perform an EMSEC inspection, after installation, but before operation.

2.13.5. Correct all deficiencies identified by an EMSEC inspection and request a re-inspection.

2.13.6. Maintain countermeasures to as-applied or as-installed conditions.

2.13.7. Initiate requests for temporary and permanent waivers (see paragraph **13.**) and EMSEC tests (AFMAN 33-214, Volume 2, [will become AFI 33-203, Volume 3]), when needed.

2.14. SPECAT Facilities. Facilities that process SPECAT classified information are administered outside the normal chain of command. SPECAT EMSEC management offices are:

2.14.1. Office of the Secretary of the Air Force (SAF/AQ-PJ). Administers EMSEC guidance and fulfills the responsibilities of the MAJCOM IA office for all special access required and special access programs accredited facilities (see paragraph **2.9.**).

2.14.2. Defense Intelligence Agency (DIA/DAC-2A). Provides EMSEC guidance and fulfills the responsibilities of the MAJCOM IA office for all DIA accredited Sensitive Compartmented Information (SCI) facilities (see paragraph **2.9.**).

2.14.3. HQ AIA/DOXC. Provides EMSEC guidance and fulfills the responsibilities of the MAJCOM IA office for all National Security Agency (NSA) accredited SCIFs under Air Force control (see paragraph **2.9.**).

2.14.4. For all other SPECAT facilities, contact HQ AFCA/EVPI AF-CTTA for guidance.

3. The Emission Security Process. An important part of IA is the certification and accreditation (C&A) process. The C&A process addresses vulnerabilities and threats with the goal of reducing the risk to an acceptable level. EMSEC is part of the C&A process. For more information on the C&A process, refer to AFI 33-202, Volume 1, *Network and Computer Security* (Chapter 6 will become AFI 33-202, Volume 2, *Certification and Accreditation*). The EMSEC process determines protective measures that will deny unauthorized personnel access to classified information and information collected from the intercept and analysis of emanations from information systems processing classified information. Air Force organizations and contractors doing business as the Air Force, whether procuring or using information systems to process classified information, must apply EMSEC proportional to the threat of exploitation. They must consider the potential damage to national security if classified information is compromised. Following are the major steps and where they fit into the C&A process.

3.1. The user contacts the wing IA office whenever they intend to process classified information. The user must do this before selecting the operational facility or room, beginning architectural engineering and facility design, procuring information systems, beginning engineering and installation, or processing classified information. See **Attachment 2** for an EMSEC flowchart.

3.2. The wing IA office determines required IA countermeasures and makes the EMSEC assessments to determine the need for EMSEC countermeasures (see paragraph **4.**). When needed, the wing IA office makes the EMSEC countermeasures reviews to determine specific EMSEC countermeasures based on the threat for that location (see paragraph **5.**). This is the EMSEC portion of determining the security policy for the C&A of the information system.

3.3. The selection of EMSEC countermeasures is validated by the Air Force CTTA (see paragraph **6.**).

3.4. The required countermeasures are given to the user for application or implementation (see paragraph **7.**).

3.5. The wing IA office inspects the application of countermeasures for correctness and effectiveness (see paragraph **8.**). The inspection is made during the security test and evaluation task of the C&A.

3.6. The wing IA office certifies the information system meets EMSEC requirements as part of the certification phase of the C&A (see paragraph **9.**).

3.7. Processing classified information without complying with the above requirements is a reportable security incident under AFI 31-401, *Information Security Program Management*, except as allowed for by waiver in paragraph **13.**

4. Emission Security Assessments . EMSEC assessments determine if the threat is sufficient to require EMSEC countermeasures reviews. This process determines the IA countermeasures and the need for EMSEC countermeasures for an information system that will process classified information.

4.1. The using Air Force organization determines if the information system will process classified information.

4.2. If the information system will process classified information, the using organization must contact the wing IA office.

4.2.1. The IA office makes the EMSEC assessments for all information systems that process classified information.

4.2.2. The MAJCOM IA office determines EMSEC requirements for MAJCOM-level programs through the subordinate wing IA offices.

4.2.3. The lead MAJCOM IA office or the CTTA determines the EMSEC requirements for Air Force-level programs through the MAJCOM IA offices.

4.2.4. For SPECAT information, the CTTA determines the EMSEC requirements.

4.3. All IA offices:

4.3.1. Use AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]) to determine required IA countermeasures and make the EMSEC assessments.

4.3.2. Document the IA countermeasures and the EMSEC assessments on AF IMT 4170, ***(S) Emission Security Assessments (U)/Emission Security Countermeasures Reviews***, according to AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]).

4.3.3. Verify the basic assessment data (equipment, location, and classification level) annually. Document this as a note, dated and signed, on the AF Form 4170 for the information system. This may be done by telephone.

5. Emission Security Countermeasures Reviews . This process determines the needed EMSEC countermeasures for an information system that will process classified information.

5.1. If the EMSEC assessments determine the need for EMSEC countermeasures, make the appropriate countermeasures reviews according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

5.2. Document the EMSEC countermeasure reviews on AF IMT 4170 according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3). Use the same form/IMT used for the EMSEC assessments.

6. Validation Requirements. The CTTA must validate the EMSEC countermeasures reviews because of the costs involved in applying countermeasures to some facilities and the cost of some countermeasures. Validate EMSEC countermeasures reviews according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

7. Applying Countermeasures . The user applies or implements the required IA and EMSEC countermeasures. Notify the wing IA office when completed.

8. Emission Security Inspection . Upon notification from the user, the wing IA office makes an EMSEC inspection to make sure the required IA and EMSEC countermeasures are effectively applied or implemented. The documented EMSEC assessments and countermeasures reviews are the basis for the EMSEC inspection. The user must correct deficiencies discovered by an EMSEC inspection or request a temporary or permanent waiver before processing classified information. While operating under a temporary

waiver, the system can only operate under interim approval. Reinspect during reassessments (see paragraph **11.**).

9. Emission Security Certification. As a part of the C&A process, the wing IA office certifies all required EMSEC countermeasures are in place after the EMSEC inspection. Certify the information system as meeting EMSEC requirements on AF IMT 4170 according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3). Recertify during reassessments (see paragraph **11.**). Document recertification by dating and signing the AF IMT 4170 in or near the certification block.

10. Maintaining Emission Security Countermeasures . The user must maintain the IA and EMSEC countermeasures to the as-certified condition. If equipment is moved or added in an area where classified information is processed, whether the moved or added equipment processes classified information or not, it must be done meeting the established IA and EMSEC countermeasures.

11. Reassessing Requirements . Reassess EMSEC requirements when required by a computer security (COMPUSEC) risk analysis (at least every three years), the EMSEC threat changes, or when the classification level of the information changes. Make a reassessment by reviewing and confirming the documented information. You do not need a new AF Form 4170 for changes, such as equipment, office, room, or building changes that do not change the outcome of the EMSEC assessments or countermeasures reviews. Make pen and ink changes instead. If the AF Form 4170 gets too messy, re-accomplish the form. Document reassessments by dating and signing the AF Form 4170 in or near the authentication and acknowledgement block of the AF Form 4170.

12. Emission Security Information Messages. ESIMs are issued by the Air Force CTTA to make time-critical changes to the Air Force EMSEC process and publications, update requirements, and clarify guidance. Compliance with ESIMs is mandatory since they augment this instruction; AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]); and AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

13. Waivers . There are two kinds of EMSEC waivers: Temporary and Permanent.

13.1. AF Form 4169, **Request for Waiver from Information Assurance Criteria**. Use this form to document and request either a temporary (see **Attachment 3**) or permanent waiver (see **Attachment 4**). A separate form is required for each countermeasure to be waived.

13.2. Filing. A copy of each temporary or permanent waiver must be filed with the documentation of the EMSEC assessments and countermeasures reviews.

13.3. Temporary Waiver. A temporary waiver allows the processing of classified information when the user is not able to implement or apply a required IA or EMSEC countermeasure. A temporary waiver is valid for one year to allow the user to accomplish the mission while they implement or apply required IA or EMSEC countermeasures.

13.3.1. Conditions. The following conditions must exist before processing a temporary waiver:

13.3.1.1. A required IA or EMSEC countermeasure was not installed or applied during installation.

13.3.1.2. Operation is required for mission accomplishment.

13.3.1.3. The user cannot implement required IA or EMSEC countermeasures before system turn-on.

13.3.2. Processing a Temporary Waiver. The user originates the request for a temporary waiver according to **Attachment 3** using AF Form 4169, and then sends it to the wing IA office for coordination and approval or disapproval by the appropriate authority.

13.3.2.1. For IA and EMSEC information systems countermeasures.

13.3.2.1.1. For collateral information, the approval authority for the temporary waiver is the designated approval authority (DAA). Forward a copy of the approved waiver, including renewals and cancellations, to the MAJCOM IA office and HQ AFCA/EVPI AF-CTTA.

13.3.2.1.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC Manager to the SPECAT DAA.

13.3.2.1.3. For Global Command and Control System (GCCS) information, process the temporary waiver through the MAJCOM IA office to the GCCS DAA.

13.3.2.2. For EMSEC communications systems and cryptographic equipment countermeasures, the CTTA approves all temporary waivers.

13.3.2.2.1. For collateral information, the approval authority is the Air Force CTTA.

13.3.2.2.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC representative to HQ AFCA/EVPI AF-CTTA.

13.3.2.2.3. For GCCS information, process the temporary waiver through the MAJCOM IA office to HQ AFCA/EVPI AF-CTTA.

13.3.3. Temporary Waiver Renewals. A one-year temporary waiver is renewable only if the user is making an active effort to correct the problem; otherwise do not renew it. Process a renewal according to paragraph **13.3.2.** before the current temporary waiver expires. After the initial temporary waiver, only two additional renewals are permitted. Waivers will not exceed a cumulative period of three years. After three years, the information system loses its interim approval to operate.

13.3.4. Temporary Waiver Cancellations. Cancel the temporary waiver after applying the required IA or EMSEC countermeasure (see **Attachment 3** for instructions).

13.4. Permanent Waiver. Only a CTTA may permanently waive a specific IA or EMSEC countermeasure. Such things as an extremely low volume of classified information, a low level of classification, disproportionate costs, impossible to do, or other conditions that make the application of the IA or EMSEC countermeasure seem inappropriate to the wing IA office, are the basis for a permanent waiver. Permanent waivers have no expiration date and are valid as long as the conditions for approval do not change. Such things as moving equipment will invalidate a permanent waiver. Review permanent waivers when making a reassessment of EMSEC requirements. Process requests as follows:

13.4.1. The user initiates the request and forwards it to the IA office for review.

13.4.2. The IA office reviews the request for validity and, if valid, forwards the request to the MAJCOM IA office or SPECAT EMSEC representative for review.

13.4.3. The MAJCOM IA office or SPECAT EMSEC representative reviews the request and, if valid, forwards it, along with appropriate supportive comments, to HQ AFCA/EVPI AF-CTTA for approval or disapproval by the CTTA.

14. Certified TEMPEST Technical Authority . A CTTA is an experienced, technically qualified government employee who meets established certification requirements according to CNSS-approved criteria and appointed by HQ USAF/XICIA to fulfill CTTA responsibilities. A CTTA conducts or validates countermeasures reviews to determine compliance with applicable national, Department of Defense (DoD), and Air Force policy and instructions. A CTTA must meet the following requirements:

14.1. Complete three continuous years of EMSEC technical experience, including at least one year of experience evaluating vulnerabilities of operational facilities and recommending countermeasures. This requirement cannot be waived.

14.2. Complete mandatory training on the technical threat. This requirement cannot be waived.

14.3. Complete technical training identified by the CNSS. Only HQ USAF/XICIA may waive technical training requirements.

15. Information Collections, Records, and Forms .

15.1. Information Collections. No information collection requirements are created by this publication.

15.2. Records. No records requirements are created by this publication.

15.3. Forms (Adopted and Prescribed).

15.3.1. Adopted Forms. AF Form 847, **Recommendation for change of Publication** and AF Form 4170, **Emission Security Assessments/Emission Security Countermeasures Reviews**.

15.3.2. Forms Prescribed. AF Form 4169**, Request For Waiver From Information Assurance Criteria**.

WILLIAM T. HOBBINS, Lt Gen, USAF
DCS, Warfighting Integration
Acting Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 31-401, *Information Security Program Management*

AFI 33-201, Volume 1, (FOUO) Communications Security (COMSEC)

AFI 33-202, Volume 1, *Network and Computer Security* (Chapter 6 will become AFI 33-202, Volume 2, *Certification and Accreditation*)

AFI 33-204, *Information Assurance (IA) Awareness Program* (will become *Information Assurance (IA) Education, Training, and Awareness Program*

AFI 36-2201, *Developing, Managing, and Conducting Training*

AFDIR 33-303, *Compendium of Communications and Information Technology*

AFMAN 10-401, Volume 1, *Operation Plan and Concept Plan Development and Implementation*

AFMAN 33-214, Volume 1, (S) *Emission Security Assessments (U)* (will become AFI 33-203, Volume 2 [S])

AFMAN 33-214, Volume 2, Emission Security Countermeasures and Reviews (will become AFI 33-203, Volume 3)

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

NSTISSAM TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetic," dated 15 December 1992, Level I

AFRIMS, *Records Disposition Schedule (RDS)*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AF—Air Force (used on forms/IMTs only)

AFCA—Air Force Communications Agency

AFCESA—Air Force Civil Engineer Support Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

AIA—Air Intelligence Agency

ANG—Air National Guard

C&A—Certification and Accreditation

CNSS—Committee on National Security Systems (formerly the National Security Telecommunications and Information Systems Security Committee)

COMSEC—Communications Security

COMPUSEC—Computer Security

CTTA—Certified TEMPEST Technical Authority

DAA—Designated Approval Authority

DOD—Department of Defense

DRU—Direct Reporting Unit

E-mail—electronic mail

EMSEC—Emission Security

ESIM—Emission Security Information Message

FOA—Field Operating Agency

GCCS—Global Command and Control System

IA—Information Assurance

JP—Joint Publication

MAJCOM—Major Command

MNS—Mission Need Statement

NSA—National Security Agency

NSTISSAM—National Security Telecommunications and Information Systems Security Advisory Memorandum

PMO—Program Management Office

PSA—Project Support Agreement

RFI—Radio Frequency Interference

SAF—Secretary of the Air Force

SCI—Sensitive Compartmented Information

SPECAT—Special Category

USAF—United States Air Force

USAFR—United States Air Force Reserve

Terms

Accreditation—Formal declaration by the designated approval authority (DAA) that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on implementation of an approved set of technical, managerial and procedural safeguards.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Collateral Information—All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., Sensitive Compartmented Information) are not formally established.

Compromising Emanation—Unintentional signal that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information-processing equipment.

Countermeasures—1. That form of military science that by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. 2. Any action, device, procedure, technique, or other means that reduces the vulnerability of an information system.

Emanation—Unintended signals or noise appearing external to an equipment.

Emission Security (EMSEC)—The protection resulting from all measures taken to deny unauthorized personnel information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic-equipment, information systems, and telecommunications systems.

EMSEC Assessment—A desktop analysis to determine whether an EMSEC countermeasures review is required or not. There are separate EMSEC assessments for information systems, communications systems, and cryptographic equipment.

EMSEC Countermeasures Review—A technical evaluation of a facility where classified information will be processed that identifies the EMSEC vulnerabilities and threats, specifies the required inspectable space, determines the required EMSEC countermeasures, and ascertains the most cost-effective way to apply required countermeasures.

Facility—1. A real-property entity consisting of one or more of the following: a building; a structure; a utility system, pavement, and underlying land. 2. A physically definable area that contains classified information-processing equipment.

Information Systems—Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. ***(NOTE):*** This includes automated information systems.

Inspectable Space—The three-dimensional space surrounding equipment that processes classified national security or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify or remove a potential TEMPEST exploitation exists.

Special Category (SPECAT) Information—The definition of SPECAT is classified (see AFMAN

33-214, Volume 1, *(S) Emission Security Assessments (U)* (will become AFI 33-203, Volume 2, (S) *Emission Security Assessments (U)*).

TEMPEST—An unclassified term referring to technical investigations for compromising emanations from electrically operated processing equipment; these investigations are conducted in support of emission security.

TEMPEST-Certified Equipment—Information systems or equipment that were certified within the requirements of the effective edition of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetic," dated 15 December 1992, Level I; or TEMPEST specifications as determined by the department or agency concerned.

Attachment 2

THE EMISSION SECURITY FLOW CHART

A2.1. Use the flowcharts in **Figure A2.1.** and **Figure A2.2.** to assess equipment and facilities to determine the need for EMSEC; determine, validate, and implement or apply the required countermeasures; and periodically reassess EMSEC requirements.

Figure A2.1. The Emission Security Flowchart.

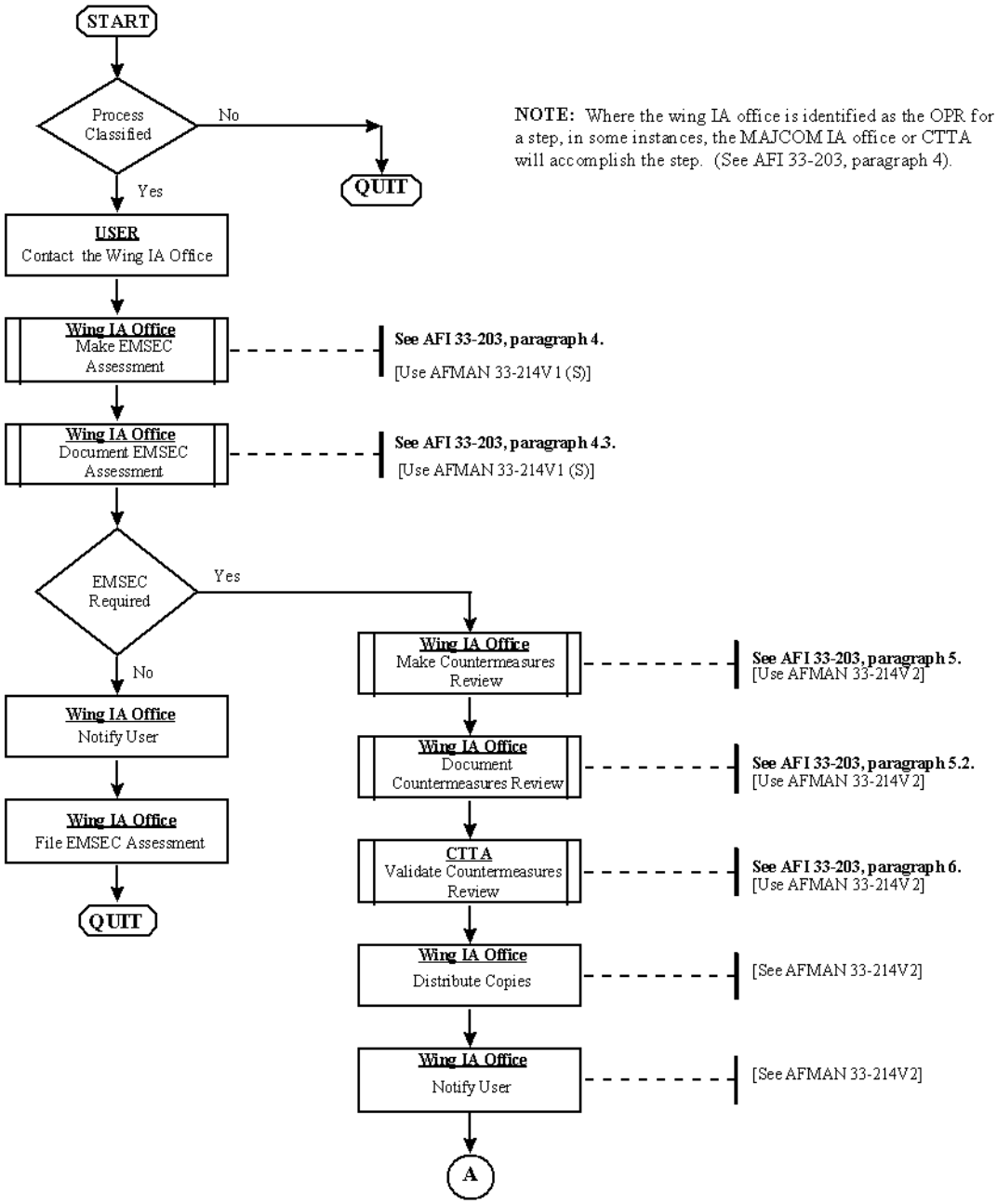
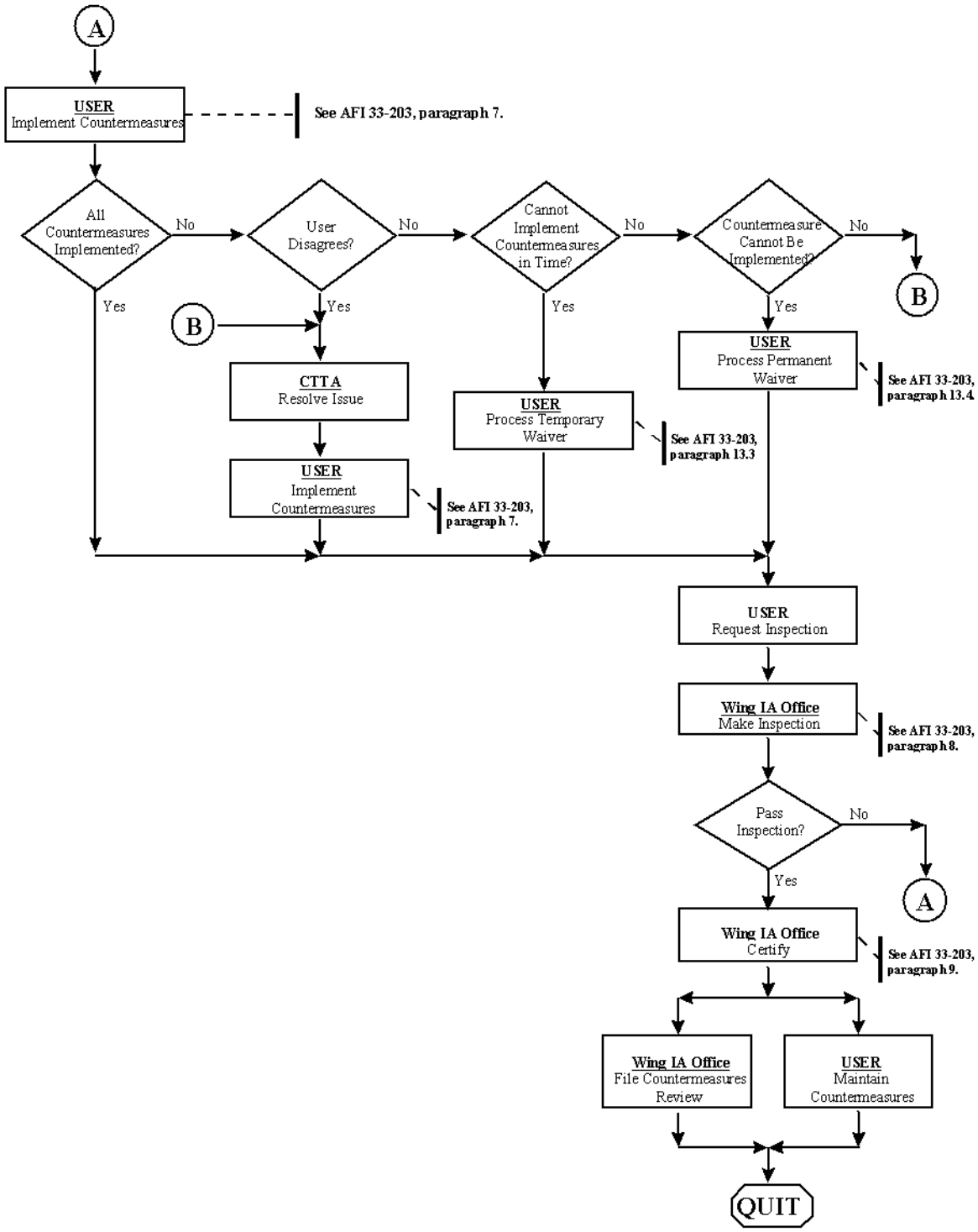


Figure A2.2. The Emission Security Flowchart Continued.



Attachment 3

PROCEDURES FOR REQUESTING A TEMPORARY WAIVER FROM INFORMATION ASSURANCE CRITERIA

A3.1. Temporary Waiver . This attachment provides guidance for completing AF Form 4169 for a temporary waiver to an EMSEC requirement. Due to the limited space on the AF Form 4169, attach additional information as required.

A3.2. Filling Out the Form for Collateral Information .

A3.2.1. Block 1: The wing IA office numbers the initial temporary waiver using the following format: MAJCOM, base, requesting unit, three-digit temporary waiver number with a "T". Use the original temporary waiver number for renewals. EXAMPLES: ACC-Langley-1CS-001T, AFMC-Edwards-95CS-104T.

A3.2.2. Block 2: Not to exceed one year from the date of approval (Block 30).

A3.2.3. TO: Either a senior manager in the user's chain to the DAA or the wing IA office; use organization and office symbol.

A3.2.4. FROM: The requester's organization and office symbol.

A3.2.5. Block 3: Check "temporary" and either "initial," "renewal," or "cancellation." ***NOTE:*** For cancellations: skip Blocks 4 through 6 and 8 through 18.

A3.2.6. Block 4: Base, building, room number, organization, office symbol, and title.

A3.2.7. Block 5: List the specific countermeasure not met.

A3.2.8. Block 6: State the problem briefly. If the approving authority will need more information than will fit in the block to fully understand the problem, use plain bond paper and attach the continued discussion.

A3.2.9. Block 7: Briefly explain your justification for processing classified information without applying or implementing a required countermeasure. For example, what is the mission impact of not processing? Why can't you apply the countermeasure before system turn-on? Attach a copy of the EMSEC countermeasures reviews.

A3.2.9.1. For Renewals: The first entry in Block 7 must be, "The initial temporary waiver approved date is ____."

A3.2.9.2. For Cancellations: Explain the cancellation. For example, "countermeasure applied" or "equipment no longer used to process classified information."

A3.2.10. Block 8:

A3.2.10.1. Initial: List interim procedures to lessen the risk while the temporary waiver is in effect.

A3.2.10.2. Renewal: Indicate the corrective actions you have taken to date.

A3.2.11. Block 9:

A3.2.11.1. Initial: State the action that will correct the deficiency. State the date corrective measures will start. State the completion date for corrective measures.

A3.2.11.2. Renewal: State what corrective actions remain. State the date remaining corrective measures will start. State the completion date for remaining corrective measures.

A3.2.12. Blocks 10 and 11: Self explanatory.

A3.2.13. Block 12: As necessary within the requester's organization.

A3.2.14. Blocks 13 through 15: Self explanatory.

A3.2.15. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the IA office is mandatory. It is the last review before forwarding the request to the DAA. You can have no more than two reviews.

A3.2.16. First Reviewing Official.

A3.2.16.1. TO: The wing IA office.

A3.2.16.2. FROM: This reviewer (organization and office symbol); either a manager in the user's chain or the IA office.

A3.2.16.3. Block 16: As necessary within the reviewer's organization.

A3.2.16.4. Block 17: Self explanatory.

A3.2.16.5. Block 18: Mark the "approval" or "disapproval" block.

A3.2.16.6. Blocks 19 through 21: Self explanatory.

A3.2.17. The Wing IA Office's Review.

A3.2.17.1. TO: The DAA.

A3.2.17.2. FROM: The wing IA office (organization and office symbol).

A3.2.17.3. Block 16 or 22: As necessary within the IA office.

A3.2.17.4. Block 17 or 23: Self explanatory.

A3.2.17.5. Block 18 or 24: Mark the "approval" or "disapproval" block.

A3.2.17.6. Blocks 19 through 21 or 25 through 27: Self explanatory.

A3.2.18. Approval Authority: Use this area to approve the temporary waiver.

A3.2.18.1. TO: The requester (organization and office symbol).

A3.2.18.2. FROM: The DAA.

A3.2.18.3. Block 28: As necessary.

A3.2.18.4. Block 29: Mark the "approved" or "disapproved" or "returned for further action" block.

A3.2.18.5. Block 30: The date this form is signed is the date of approval.

A3.2.18.6. Blocks 31 and 32: Self explanatory.

A3.2.19. Block 33: The originator places the “classified by” and “declassify on” in the bottom right corner of this block.

A3.3. Filling Out the Form for Special Category Information .

A3.3.1. Complete all of paragraphs **A3.2.1.** through **A3.2.14.**, and **A3.2.19.**

A3.3.2. In the first TO: block after Block 2, add the base to the organization and office symbol.

A3.3.3. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IA office and the SPECAT EMSEC representative is mandatory and is the last review before forwarding the request to the approving authority. If you need reviews in addition to the IA office and SPECAT EMSEC person, attach additional AF Forms 4169 using only the reviewing official blocks.

A3.3.4. Reviewing Official Other Than The Wing IA Office. Any manager in the user’s chain.

A3.3.4.1. TO: The next level for review or the wing IA office (organization, office symbol, and base).

A3.3.4.2. FROM: This reviewer (organization, office symbol, and base).

A3.3.4.3. Block 16: As necessary within the reviewer’s organization.

A3.3.4.4. Block 17: Self explanatory.

A3.3.4.5. Block 18: Mark the “approval” or “disapproval” block.

A3.3.4.6. Blocks 19 through 21: Self explanatory.

A3.3.5. The Wing IA Office’s Review.

A3.3.5.1. TO: The SPECAT EMSEC person (organization, office symbol, and base).

A3.3.5.2. FROM: The wing IA office (organization, office symbol, and base).

A3.3.5.3. Block 16: As necessary within the wing IA office.

A3.3.5.4. Block 17: Self explanatory.

A3.3.5.5. Block 18: Mark the “approval” or “disapproval” block.

A3.3.5.6. Blocks 19 through 21: Self explanatory.

A3.3.6. The SPECAT EMSEC Representative’s Review.

A3.3.6.1. TO: The SPECAT information DAA (organization, office symbol, and base).

A3.3.6.2. FROM: The SPECAT EMSEC person (organization and office symbol).

A3.3.6.3. Block 16: As necessary within the SPECAT EMSEC person's office.

A3.3.6.4. Block 17: Self explanatory.

A3.3.6.5. Block 18: Mark the “approval” or “disapproval” block.

A3.3.6.6. Blocks 19 through 21: Self explanatory.

A3.3.7. Approval Authority: This area is used to approve the temporary waiver.

A3.3.7.1. TO: The requester (organization, office symbol, and base).

A3.3.7.2. FROM: The SPECAT information DAA (organization, office symbol, and base).

A3.3.7.3. Block 28: As necessary.

A3.3.7.4. Block 29: Mark the “approved” or “disapproved” or “returned for further action” block.

A3.3.7.5. Block 30: The date this form is signed is the date of approval.

A3.3.7.6. Blocks 31 and 32: Self explanatory.

Attachment 4

PROCEDURES FOR REQUESTING A PERMANENT WAIVER FROM INFORMATION ASSURANCE CRITERIA

A4.1. Permanent Waiver. This attachment provides guidance for completing the AF Form 4169 for a permanent waiver to an EMSEC requirement. Due to the limited space on the AF Form 4169, attach additional information as required.

A4.2. Filling Out the Form for Collateral Information.

A4.2.1. Block 1: The wing IA office numbers the initial permanent waiver using the following format: MAJCOM, base, requesting unit, three-digit permanent waiver number with a "P." EXAMPLES: ACC-Langley-1CS-001P, AFMC-Edwards-95CS-104P.

A4.2.2. Block 2: Enter, "No expiration date."

A4.2.3. TO: Either the DAA or the wing IA office; use organization and office symbol.

A4.2.4. FROM: The requester's organization and office symbol.

A4.2.5. Block 3: Check "permanent" and either "initial or "cancellation." ***NOTE:*** For cancellations: skip Blocks 4 through 6 and 8 through 18.

A4.2.6. Block 4: Base, building, room number, organization, office symbol, and title.

A4.2.7. Block 5: List the specific countermeasure not met.

A4.2.8. Block 6: State the problem briefly. If the CTTA will need more information to fully understand the problem, use an attachment and explain thoroughly.

A4.2.9. Block 7: Briefly explain your justification for processing classified information without applying the required countermeasure. For example, why can't the required countermeasure be applied? Attach a copy of the countermeasures review, AF Form 4170.

A4.2.9.1. For Cancellations: Explain the cancellation. For example, "countermeasure applied" or "equipment no longer used to process classified information."

A4.2.10. Block 8: List procedures to lessen the risk while the permanent waiver is in effect.

A4.2.11. Blocks 9 through 11: Leave blank.

A4.2.12. Blocks 12: As necessary within the requester's organization.

A4.2.13. Blocks 13 through 15: Self-explanatory.

A4.2.14. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing and MAJCOM IA offices is mandatory. It is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing and MAJCOM IA offices, attach additional AF Forms 4169 using only the reviewing official blocks.

A4.2.15. Reviewing Official Other Than The Wing IA Office. Any manager in the user's chain.

A4.2.15.1. TO: The next level for review or the wing IA office (organization, office symbol, and base).

A4.2.15.2. FROM: This reviewer (organization, office symbol, and base).

A4.2.15.3. Block 16: As necessary within the reviewer's organization.

A4.2.15.4. Block 17: Self-explanatory.

A4.2.15.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.15.6. Blocks 19 through 21: Self-explanatory.

A4.2.16. The Wing IA Office's Review.

A4.2.16.1. TO: The MAJCOM IA office (organization, office symbol, and base).

A4.2.16.2. FROM: The wing IA office (organization, office symbol, and base).

A4.2.16.3. Block 16: As necessary within the wing IA office.

A4.2.16.4. Block 17: Self-explanatory.

A4.2.16.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.16.6. Blocks 19 through 21: Self-explanatory.

A4.2.17. The MAJCOM IA Office's Review.

A4.2.17.1. TO: The CTTA (organization, office symbol, and base).

A4.2.17.2. FROM: The MAJCOM IA office (organization and office symbol).

A4.2.17.3. Block 16: As necessary within the MAJCOM IA office.

A4.2.17.4. Block 17: Self-explanatory.

A4.2.17.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.17.6. Blocks 19 through 21: Self-explanatory.

A4.2.18. Approval Authority: The CTTA uses this area to approve the waiver request.

A4.2.18.1. TO: The requester, organization, and office symbol.

A4.2.18.2. FROM: CTTA, HQ AFCA/EVPI.

A4.2.18.3. Block 28: As necessary.

A4.2.18.4. Block 29: Mark the "approved" or "disapproved" or "returned for further action" block.

A4.2.18.5. Block 30: The date this form is signed is the date of approval.

A4.2.18.6. Blocks 31 and 32: Self-explanatory.

A4.2.19. Block 33: The originator places the "Classified by:" and "Declassify on:" on the bottom right corner of this block.

A4.3. Filling Out the Form for Special Category Information.

A4.3.1. Complete all of paragraphs **A4.2.1.** through **A4.2.14.**, and **A4.2.19.**

A4.3.2. In the first TO: block after Block 2, add the base to the organization and office symbol.

A4.3.3. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IA office and the SPECAT EMSEC person is mandatory and is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing IA office and SPECAT EMSEC person, attach additional AF Forms 4169 using only the reviewing official blocks.

A4.3.4. Reviewing Official Other Than The Wing IA Office. Any manager in the user's chain.

A4.3.4.1. TO: The next level for review or the wing IA office (organization, office symbol, and base).

A4.3.4.2. FROM: This reviewer (organization, office symbol, and base).

A4.3.4.3. Block 16: As necessary within the reviewer's organization.

A4.3.4.4. Block 17: Self-explanatory.

A4.3.4.5. Block 18: Mark the "approval" or "disapproval" block.

A4.3.4.6. Blocks 19 through 21: Self-explanatory.

A4.3.5. The Wing IA Office's Review.

A4.3.5.1. TO: The SPECAT EMSEC representative (organization, office symbol, and base).

A4.3.5.2. FROM: The wing IA office (organization, office symbol, and base).

A4.3.5.3. Block 16: As necessary within the wing IA office.

A4.3.5.4. Block 17: Self-explanatory.

A4.3.5.5. Block 18: Mark the "approval" or "disapproval" block.

A4.3.5.6. Blocks 19 through 21: Self-explanatory.

A4.3.6. The SPECAT EMSEC Representative's Review.

A4.3.6.1. TO: The CTTA (organization, office symbol, and base).

A4.3.6.2. FROM: The SPECAT EMSEC representative (organization and office symbol).

A4.3.6.3. Block 16: As necessary within the SPECAT EMSEC representative's office.

A4.3.6.4. Block 17: Self-explanatory.

A4.3.6.5. Block 18: Mark the "approval" or "disapproval" block.

A4.3.6.6. Blocks 19 through 21: Self-explanatory.

A4.3.7. Approval Authority: This area is used to approve the permanent waiver.

A4.3.7.1. TO: The requester (organization, office symbol, and base).

A4.3.7.2. FROM: The CTTA (organization, office symbol, and base).

A4.3.7.3. Block 28: As necessary.

A4.3.7.4. Block 29: Mark the "approved" or "disapproved" or "returned for further action" block.

A4.3.7.5. Block 30: The date this form is signed is the date of approval.

A4.3.7.6. Blocks 31 and 32: Self-explanatory.

Attachment 5

INTERIM CHANGE (IC) 2005-1 TO AFI 33-203, EMISSION SECURITY

31 OCTOBER 2005

AIR FORCE INSTRUCTION 33-203, VOLUME 1

OPR: HQ AFCA/EVPI (Mr. Cyril Prikazsky)

Certified by: SAF/XCIA (Mr. David G. Ferguson)

This Air Force instruction (AFI) implements the emission security (EMSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and establishes Air Force information assurance (IA) countermeasures and EMSEC requirements for IA. It interfaces with AFI 33-201, Volume 1, *(FOUO) Communications Security (COMSEC)*; AFI 33-202, Volume 1, *Network and Computer Security*; and AFI 33-204, *Information Assurance Awareness Program* (will become AFI 33-204, *Information Assurance Education, Training, and Awareness Program*). This instruction applies to all Air Force military, civilians, and contractor personnel under contract by the Department of Defense (DOD) that participate in the emission security program. This instruction applies to the Air National Guard (ANG). We encourage the use of extracts from this instruction. Additional security instructions and manuals are listed on the Air Force website at **http://www.e-publishing.af.mil** under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this instruction, through appropriate channels, to HQ Air Force Communications Agency (HQ AFCA/EVPI AF-CTTA), 203 W. Losey Street, Room 2000, Scott AFB IL 62225-5222, or the EMSEC organizational E-mail box at **afca.ctta.emsec@scott.af.mil**. Refer recommended changes and conflicts between this and other publications to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force (AF) IMT 847, **Recommendation for Change of Publication**. Send an information copy to Secretary of the Air Force (SAF/XCIA), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363), and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds/index.cfm**. See **Attachment 1** for a glossary of references and supporting information used in this instruction.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2005-01 (**Attachment 5**). Upon incorporation of IC 2005-1, the number of this publication changes from AFI 33-203, *Emission Security* to AFI 33-203, Volume 1, *Emission Security*, to comply with Air Staff's direction to align all EMSEC publications to be under the AFI 33-203 umbrella. It updates office symbols, changes some forms to IMTs, and updates publications throughout the entire instruction. A bar (|) indicates a revision from the previous edition.

1.1. The objective of EMSEC is to deny access to classified and, in some instances, unclassified information and contain compromising emanations within an inspectable space. Instances of when you must consider unclassified information are addressed in AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)* (will become AFI 33-203, Volume 2 *(S), Emission Security Assessments (U)*). The term "classified information," as used in this instruction, includes those instances. This is accomplished by

identifying requirements from the broader view of IA and providing the appropriate protection at the least possible cost. Key to this is a partnership between the IA office and the user.

2.3.3. Work with HQ AFCA/EVPI AF-CTTA to make sure EMSEC portions of curriculums are current and meet Air Force needs.

2.4.9. Coordinates exchange of engineering and installation EMSEC information with HQ AFCA/EVPI AF-CTTA.

2.11.9. Forwards a copy of all EMSEC countermeasures reviews according to AFMAN 33-214, Volume 2, *Emission Security Countermeasures Reviews* (will become AFI 33-203, Volume 3, *Emission Security Countermeasures Reviews*).

2.13.7. Initiate requests for temporary and permanent waivers (see paragraph **13.**) and EMSEC tests (AFMAN 33-214, Volume 2, [will become AFI 33-203, Volume 3]), when needed.

2.14.4. For all other SPECAT facilities, contact HQ AFCA/EVPI AF-CTTA for guidance.

3. **The Emission Security Process.** An important part of IA is the certification and accreditation (C&A) process. The C&A process addresses vulnerabilities and threats with the goal of reducing the risk to an acceptable level. EMSEC is part of the C&A process. For more information on the C&A process, refer to AFI 33-202, Volume 1, *Network and Computer Security* (Chapter 6 will become AFI 33-202, Volume 2, *Certification and Accreditation*). The EMSEC process determines protective measures that will deny unauthorized personnel access to classified information and information collected from the intercept and analysis of emanations from information systems processing classified information. Air Force organizations and contractors doing business as the Air Force, whether procuring or using information systems to process classified information, must apply EMSEC proportional to the threat of exploitation. They must consider the potential damage to national security if classified information is compromised. Following are the major steps and where they fit into the C&A process.

4.3.1. Use AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]) to determine required IA countermeasures and make the EMSEC assessments.

4.3.2. Document the IA countermeasures and the EMSEC assessments on AF IMT 4170, ***(S) Emission Security Assessments (U)/Emission Security Countermeasures Reviews***, according to AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]).

5.1. If the EMSEC assessments determine the need for EMSEC countermeasures, make the appropriate countermeasures reviews according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

5.2. Document the EMSEC countermeasure reviews on AF IMT 4170 according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3). Use the same form/IMT used for the EMSEC assessments.

6. **Validation Requirements.** The CTTA must validate the EMSEC countermeasures reviews because of the costs involved in applying countermeasures to some facilities and the cost of some countermeasures. Validate EMSEC countermeasures reviews according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

9. **Emission Security Certification.** As a part of the C&A process, the wing IA office certifies all required EMSEC countermeasures are in place after the EMSEC inspection. Certify the information system as meeting EMSEC requirements on AF IMT 4170 according to AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3). Recertify during reassessments (see paragraph **11.**). Document recertification by dating and signing the AF IMT 4170 in or near the certification block.

12. **Emission Security Information Messages.** ESIMs are issued by the Air Force CTTA to make time-critical changes to the Air Force EMSEC process and publications, update requirements, and clarify guidance. Compliance with ESIMs is mandatory since they augment this instruction; AFMAN 33-214, Volume 1 (S) (will become AFI 33-203, Volume 2 [S]); and AFMAN 33-214, Volume 2 (will become AFI 33-203, Volume 3).

13.3.2.1.1. For collateral information, the approval authority for the temporary waiver is the designated approval authority (DAA). Forward a copy of the approved waiver, including renewals and cancellations, to the MAJCOM IA office and HQ AFCA/EVPI AF-CTTA.

13.3.2.2.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC representative to HQ AFCA/EVPI AF-CTTA.

13.3.2.2.3. For GCCS information, process the temporary waiver through the MAJCOM IA office to HQ AFCA/EVPI AF-CTTA.

13.4.3. The MAJCOM IA office or SPECAT EMSEC representative reviews the request and, if valid, forwards it, along with appropriate supportive comments, to HQ AFCA/EVPI AF-CTTA for approval or disapproval by the CTTA.

WILLIAM T. HOBBINS, Lt Gen, USAF

DCS, Warfighting Integration

Acting Chief of Warfighting Integration and

Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFI 31-401, *Information Security Program Management*

AFI 33-201, Volume 1, (FOUO) Communications Security (COMSEC)

AFI 33-202, Volume 1, *Network and Computer Security* (Chapter 6 will become AFI 33-202, Volume 2, *Certification and Accreditation*)

AFI 33-204, *Information Assurance (IA) Awareness Program* (will become *Information Assurance (IA) Education, Training, and Awareness Program*

AFI 36-2201, *Developing, Managing, and Conducting Training*

AFDIR 33-303, *Compendium of Communications and Information Technology*

AFMAN 10-401, Volume 1, *Operation Plan and Concept Plan Development and Implementation*

AFMAN 33-214, Volume 1, (S) *Emission Security Assessments (U)* (will become AFI 33-203, Volume 2 [S])

AFMAN 33-214, Volume 2, Emission Security Countermeasures and Reviews (will become AFI 33-203, Volume 3)

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

NSTISSAM TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetic," dated 15 December 1992, Level I

AFRIMS, *Records Disposition Schedule (RDS)*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AF—Air Force (used on forms/IMTs only)

AFCA—Air Force Communications Agency

AFCESA—Air Force Civil Engineer Support Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

AIA—Air Intelligence Agency

ANG—Air National Guard

C&A—Certification and Accreditation

CNSS—Committee on National Security Systems (formerly the National Security Telecommunications and Information Systems Security Committee)

COMSEC—Communications Security

COMPUSEC—Computer Security

CTTA—Certified TEMPEST Technical Authority

DAA—Designated Approval Authority

DOD—Department of Defense

DRU—Direct Reporting Unit

E-mail—electronic mail

EMSEC—Emission Security

ESIM—Emission Security Information Message

FOA—Field Operating Agency

GCCS—Global Command and Control System

IA—Information Assurance

JP—Joint Publication

MAJCOM—Major Command

MNS—Mission Need Statement

NSA—National Security Agency

NSTISSAM—National Security Telecommunications and Information Systems Security Advisory Memorandum

PMO—Program Management Office

PSA—Project Support Agreement

RFI—Radio Frequency Interference

SAF—Secretary of the Air Force

SCI—Sensitive Compartmented Information

SPECAT—Special Category

USAF—United States Air Force

USAFR—United States Air Force Reserve

Terms

Accreditation—Formal declaration by the designated approval authority (DAA) that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on implementation of an approved set of technical, managerial and procedural safeguards.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Collateral Information—All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., Sensitive Compartmented Information) are not formally established.

Compromising Emanation—Unintentional signal that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information-processing equipment.

Countermeasures—1. That form of military science that by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. 2. Any action, device, procedure, technique, or other means that reduces the vulnerability of an information system.

Emanation—Unintended signals or noise appearing external to an equipment.

Emission Security (EMSEC)—The protection resulting from all measures taken to deny unauthorized personnel information of value that might be derived from communications systems and cryptographic equipment intercepts and the interception and analysis of compromising emanations from cryptographic-equipment, information systems, and telecommunications systems.

EMSEC Assessment—A desktop analysis to determine whether an EMSEC countermeasures review is required or not. There are separate EMSEC assessments for information systems, communications systems, and cryptographic equipment.

EMSEC Countermeasures Review—A technical evaluation of a facility where classified information will be processed that identifies the EMSEC vulnerabilities and threats, specifies the required inspectable space, determines the required EMSEC countermeasures, and ascertains the most cost-effective way to apply required countermeasures.

Facility—1. A real-property entity consisting of one or more of the following: a building; a structure; a utility system, pavement, and underlying land. 2. A physically definable area that contains classified information-processing equipment.

Information Systems—Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. ***(NOTE):*** This includes automated information systems.

Inspectable Space—The three-dimensional space surrounding equipment that processes classified national security or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify or remove a potential TEMPEST exploitation exists.

Special Category (SPECAT) Information—The definition of SPECAT is classified (see AFMAN 33-214, Volume 1, *(S) Emission Security Assessments (U)* (will become AFI 33-203, Volume 2, (S) *Emission Security Assessments (U)*).

TEMPEST—An unclassified term referring to technical investigations for compromising emanations from electrically operated processing equipment; these investigations are conducted in support of emission security.

TEMPEST-Certified Equipment—Information systems or equipment that were certified within the requirements of the effective edition of National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92, "Compromising Emanations Laboratory Test Requirements, Electromagnetic," dated 15 December 1992, Level I; or TEMPEST specifications as determined by the department or agency concerned.

Attachment 4

PROCEDURES FOR REQUESTING A PERMANENT WAIVER FROM INFORMATION ASSURANCE CRITERIA

A4.1. **Permanent Waiver.** This attachment provides guidance for completing the AF Form 4169 for a permanent waiver to an EMSEC requirement. Due to the limited space on the AF Form 4169, attach additional information as required.

A4.2. **Filling Out the Form for Collateral Information.**

A4.2.1. Block 1: The wing IA office numbers the initial permanent waiver using the following format: MAJCOM, base, requesting unit, three-digit permanent waiver number with a "P." EXAMPLES: ACC-Langley-1CS-001P, AFMC-Edwards-95CS-104P.

A4.2.2. Block 2: Enter, "No expiration date."

A4.2.3. TO: Either the DAA or the wing IA office; use organization and office symbol.

A4.2.4. FROM: The requester's organization and office symbol.

A4.2.5. Block 3: Check "permanent" and either "initial or "cancellation." ***NOTE:*** For cancellations: skip Blocks 4 through 6 and 8 through 18.

A4.2.6. Block 4: Base, building, room number, organization, office symbol, and title.

A4.2.7. Block 5: List the specific countermeasure not met.

A4.2.8. Block 6: State the problem briefly. If the CTTA will need more information to fully understand the problem, use an attachment and explain thoroughly.

A4.2.9. Block 7: Briefly explain your justification for processing classified information without applying the required countermeasure. For example, why can't the required countermeasure be applied? Attach a copy of the countermeasures review, AF Form 4170.

A4.2.9.1. For Cancellations: Explain the cancellation. For example, "countermeasure applied" or "equipment no longer used to process classified information."

A4.2.10. Block 8: List procedures to lessen the risk while the permanent waiver is in effect.

A4.2.11. Blocks 9 through 11: Leave blank.

A4.2.12. Blocks 12: As necessary within the requester's organization.

A4.2.13. Blocks 13 through 15: Self-explanatory.

A4.2.14. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing and MAJCOM IA offices is mandatory. It is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing and MAJCOM IA offices, attach additional AF Forms 4169 using only the reviewing official blocks.

A4.2.15. Reviewing Official Other Than The Wing IA Office. Any manager in the user's chain.

A4.2.15.1. TO: The next level for review or the wing IA office (organization, office symbol, and base).

A4.2.15.2. FROM: This reviewer (organization, office symbol, and base).

A4.2.15.3. Block 16: As necessary within the reviewer's organization.

A4.2.15.4. Block 17: Self-explanatory.

A4.2.15.5. Block 18: Mark the "approval" or "disapproval" block.

A4.2.15.6. Blocks 19 through 21: Self-explanatory.

A4.2.16. The Wing IA Office's Review.

A4.2.16.1. TO: The MAJCOM IA office (organization, office symbol, and base).

A4.2.16.2. FROM: The wing IA office (organization, office symbol, and base).

A4.2.16.3. Block 16: As necessary within the wing IA office.

A4.2.16.4. Block 17: Self-explanatory.

A4.2.16.5. Block 18: Mark the “approval” or “disapproval” block.

A4.2.16.6. Blocks 19 through 21: Self-explanatory.

A4.2.17. The MAJCOM IA Office’s Review.

A4.2.17.1. TO: The CTTA (organization, office symbol, and base).

A4.2.17.2. FROM: The MAJCOM IA office (organization and office symbol).

A4.2.17.3. Block 16: As necessary within the MAJCOM IA office.

A4.2.17.4. Block 17: Self-explanatory.

A4.2.17.5. Block 18: Mark the “approval” or “disapproval” block.

A4.2.17.6. Blocks 19 through 21: Self-explanatory.

A4.2.18. Approval Authority: The CTTA uses this area to approve the waiver request.

A4.2.18.1. TO: The requester, organization, and office symbol.

A4.2.18.2. FROM: CTTA, HQ AFCA/EVPI.

A4.2.18.3. Block 28: As necessary.

A4.2.18.4. Block 29: Mark the “approved” or “disapproved” or “returned for further action” block.

A4.2.18.5. Block 30: The date this form is signed is the date of approval.

A4.2.18.6. Blocks 31 and 32: Self-explanatory.

A4.2.19. Block 33: The originator places the “Classified by:” and “Declassify on:” on the bottom right corner of this block.

A4.3. **Filling Out the Form for Special Category Information.**

A4.3.1. Complete all of paragraphs **A4.2.1.** through **A4.2.14.**, and **A4.2.19.**

A4.3.2. In the first TO: block after Block 2, add the base to the organization and office symbol.

A4.3.3. Reviewing Official: Use Blocks 16 through 27 as necessary to document the reviews. A review by the wing IA office and the SPECAT EMSEC person is mandatory and is the last review before forwarding the request to the CTTA. If you need reviews in addition to the wing IA office and SPECAT EMSEC person, attach additional AF Forms 4169 using only the reviewing official blocks.

A4.3.4. Reviewing Official Other Than The Wing IA Office. Any manager in the user’s chain.

A4.3.4.1. TO: The next level for review or the wing IA office (organization, office symbol, and base).

A4.3.4.2. FROM: This reviewer (organization, office symbol, and base).

A4.3.4.3. Block 16: As necessary within the reviewer’s organization.

A4.3.4.4. Block 17: Self-explanatory.

A4.3.4.5. Block 18: Mark the “approval” or “disapproval” block.

A4.3.4.6. Blocks 19 through 21: Self-explanatory.

A4.3.5. The Wing IA Office's Review.

A4.3.5.1. TO: The SPECAT EMSEC representative (organization, office symbol, and base).

A4.3.5.2. FROM: The wing IA office (organization, office symbol, and base).

A4.3.5.3. Block 16: As necessary within the wing IA office.

A4.3.5.4. Block 17: Self-explanatory.

A4.3.5.5. Block 18: Mark the "approval" or "disapproval" block.

A4.3.5.6. Blocks 19 through 21: Self-explanatory.

A4.3.6. The SPECAT EMSEC Representative's Review.

A4.3.6.1. TO: The CTTA (organization, office symbol, and base).

A4.3.6.2. FROM: The SPECAT EMSEC representative (organization and office symbol).

A4.3.6.3. Block 16: As necessary within the SPECAT EMSEC representative's office.

A4.3.6.4. Block 17: Self-explanatory.

A4.3.6.5. Block 18: Mark the "approval" or "disapproval" block.

A4.3.6.6. Blocks 19 through 21: Self-explanatory.

A4.3.7. Approval Authority: This area is used to approve the permanent waiver.

A4.3.7.1. TO: The requester (organization, office symbol, and base).

A4.3.7.2. FROM: The CTTA (organization, office symbol, and base).

A4.3.7.3. Block 28: As necessary.

A4.3.7.4. Block 29: Mark the "approved" or "disapproved" or "returned for further action" block.

A4.3.7.5. Block 30: The date this form is signed is the date of approval.

A4.3.7.6. Blocks 31 and 32: Self-explanatory.