BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE SYSTEMS SECURITY INSTRUCTION 7700
24 OCTOBER 2007

Incorporating Through Change 1, 14 APRIL 2009

Communications and Information

EMISSION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publication is available for downloading on the Information Assurance website at: https://private.afca.af.mil/ip/.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFCA/EVPI

Certified By: SAF/XCPPI
(Mr. Kenneth Brodie)
Pages: 30

★This instruction implements the Emission Security (EMSEC) program as defined in Air Force Policy Directive (AFPD) 33-2, *Information Assurance (IA)*, and its implementing departmental publications. It establishes Air Force IA countermeasures and EMSEC requirements for IA compliance with Committee on National Security Systems (CNSS) Policy No.300, *National Policy on Control of Compromising Emanations*. This instruction applies to Air Force military, civilian, and contractor personnel under contract by the Department of Defense (DoD) who develop, acquire, deliver, administer or manage Emission Security (EMSEC) for Air Force information systems. This instruction applies to the Air National Guard (ANG) and Air Force Reserve Command (AFRC). The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU). This Air Force Systems Security Instruction (AFSSI) is authorized by Air Force Instruction (AFI) 33-102, *Communications and Information Specialized Publications*. Direct questions or comments on the contents of this instruction, through appropriate command channels, to Headquarters Air Force Communications Agency (HQ AFCA/EVP), 203 W. Losey Street, Room 2100, Scott AFB IL 62225-5222. Our EMSEC electronic mail (E-mail) is AFCA.CTTA.EMSEC@scott.af.mil. Refer recommended changes and conflicts between this and other publications, through appropriate channels, to HQ AFCA/EASD, 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force (AF) Form 847, *Recommendation for Change of Publication*. Send any supplements to this publication to HQ AFCA/EVP for review, coordination, and approval prior to publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a//afrims/afrims/rims.cfm. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

This instruction replaces substantial portions of AFI 33-203, Volume 1, Emission Security (EMSEC), dated 31 October 2005.

★*SUMMARY OF CHANGES*

★This interim change (IC) updates the applies statement statement in the purpose paragraph. Paragraphs 12.3, 12.4, 12.5, 12.9, 14.6.1, 16, 17.1, 17.2, 18.1, 18.2, 19, 22, 24, and 25 were updated to clarify publication reference. The proper alignment and spacing was accomplished for paragraphs 14.1 and 14.2. An update was made to paragraph 17.3.3 to provide clarification. Attachment 1 was updated in the references and terms section. Figure A2.1 of Attachment 2 was updated to correct publication reference.

Table of Contents **Page**

Section A - General

1. Introduction. The goal of IA is to assure the availability, integrity, and confidentiality of information and information systems. The IA disciplines of communications security (COMSEC), computer security (COMPUSEC), and EMSEC are interdependent. EMSEC addresses the "confidentiality" requirement. EMSEC is one of the IA disciplines promulgated in AFPD 33-2. Compliance ensures appropriate measures are taken to protect all Air Force information systems and resources that will process classified information.

2. Applicability.

2.1. Applies to all information systems, including information system components of weapon systems, information systems that provide the management infrastructure and connections among other information systems, and networks that are used to process, store, display, transmit or protect DoD information, regardless of classification or sensitivity. This document is also binding on all users that operate, connect, or interact with information systems owned, maintained, and controlled by the DoD.

2.2. More restrictive DoD and Director of Central Intelligence Agency directive requirements governing Special Access Program information take precedence over this instruction.

2.3. This instruction is not applicable to Sensitive Compartmented Information (SCI) information systems. For SCI systems, refer to the Joint Department of Defense Intelligence Information Systems (DoDIIS)/Cryptologic SCI Information Systems Security Standards.

3. Objectives. The objective of EMSEC is to deny access to classified and, in some instances, unclassified but sensitive information and contain compromising emanations within an inspectable space. Instances of when unclassified information is to be considered are addressed in AFMAN 33-214, Volume 1, (S) *Emission Security Assessments* (U) (will become AFSSI 7701). The term "classified information," as used in this instruction, includes all these instances. This is accomplished by identifying requirements from the broader view of IA and providing the appropriate protection at the least possible cost. The key to this is a partnership between the IA office and the user. These objectives will be met by provision of safeguard and their associated control collectively known as countermeasure.

3.1. Safeguards are actions or activities taken to protect information and are an integral part of security disciplines including COMPUSEC, EMSEC, COMSEC, etc.

3.2. 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.

3.3. 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.

3.4. The CNSS used risk management principles to develop the minimum EMSEC requirements identified in this AFSSI. Since the risk has been accepted at the national level, no further risk for EMSEC can be accepted.

Section B - Organizational Roles and Responsibilities

4. Secretary of the Air Force, Policy and Resources Directorate, Policy and Compliance Division (SAF/XCPP).

4.1. Develops policies and procedures for communication enterprise operations and maintenance.

4.2. SAF/XCPP. 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) who meets the experience and training prerequisites of paragraph 27.

5. Headquarters Air Force Communications Agency (HQ AFCA). On behalf of SAF/XCPP:

5.1. Tasks Headquarters Air Education and Training Command with preparation of EMSEC Manager training. Periodically reviews this curriculum.

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

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

5.4. Maintains files of EMSEC countermeasures reviews and waivers.

5.5. Reviews national TEMPEST publications and identifies those required for issuance to Air Force activities. Publications with special applications at bases outside the US will be identified. A list of required EMSEC program publications is on the Air Force EMSEC home page, https://private.afca.af.mil/ emsec. EMSEC publications are available on the Information Assurance Community of Practice website: https://wwwd.my.af.mil/afknprod/ASPs/ docman/DOCMain.asp?Tab=0&FolderID=OO-SC-IA-01-14-1&Filter=OO-SC-IA-01.

5.6. Is assigned Air Force CTTA responsibility (see paragraph 6).

5.7. Delegates to the Air Force Intelligence, Surveillance, and Reconnaissance (AF ISR) CTTA issues regarding Sensitive Compartmented Information Facilities (SCIF).

6. Certified TEMPEST Technical Authority (CTTA).

6.1. Validates all EMSEC countermeasures reviews.

6.2. Issues Emission Security Information Messages (ESIM).

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

6.4. Tasks all Air Force EMSEC testing.

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

6.6. Provides Air Force EMSEC requirements and guidance for all Air Force aircraft.

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

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

6.9. Serves as the primary CTTA for EMSEC/TEMPEST issues at Combatant (Joint) Commands which are under the Support Responsibility of the Secretary of the Air Force. See DoD Directive (DoDD) 5100.3, *Support of the Headquarters of Combatant and Subordinate Joint Commands*.

6.10. Interacts with the assigned AF ISR Agency CTTA, who is the CTTA for SCIFs.

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

7. Air Force Intelligence, Surveillance, and Reconnaissance (AF ISR) Agency.

7.1. Nominates a CTTA for SCIFs to SAF/XCPP for appointment.

7.2. The CTTA for SCIFs will have attained the experience and training prerequisites of paragraph 27.

8. The 346th Test Squadron, under the 8th Air Force and the Air Force Information Operations Center:

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

8.2. Provides a capability to test high value Air Force systems such as special air mission aircraft and strategic systems (e.g., F-35, B-2, special access required programs, and joint programs).

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

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

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

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

9. Major Commands (MAJCOM). Includes those FOAs and DRUs who have established IA offices (see paragraph 10.1):

9.1. Establish a Command EMSEC program to be managed by the MAJCOM IA office. Appoint a Command EMSEC Manager and provide a copy of the appointment to HQ AFCA/EVPI/AF-CTTA.

9.2. Include EMSEC requirements identified by the HQ AFCA (AF-CTTA)/MAJCOM IA office in requests for proposal, specifications, statements of work, Capability Development Documents (CDD), 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 equipment specifications for EMSEC considerations and criteria.

9.3. Include EMSEC requirements when preparing the COMSEC appendix to the communications annex of operations plans according to AFI 10-401, *Air Force Operations Planning and Execution*.

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

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

10. Major Command (MAJCOM) Information Assurance (IA) Office.

10.1. Manages the Command EMSEC program according to this instruction and is the focal point for all MAJCOM EMSEC requirements.

10.2. Makes sure the individual responsible for EMSEC in the IA office receives EMSEC manager training currently offered at Keesler AFB MS.

10.3. Provides EMSEC guidance and assistance to the command staff and subordinate IA offices. Include those ANG and AFRC units gained by the MAJCOM upon activation.

10.4. Implements ESIMs.

10.5. Assists wing IA offices when requested. Include those ANG and AFRC units gained by the MAJCOM upon activation.

10.6. Ensures inspection of all MAJCOM facilities that have EMSEC requirements (see paragraph 21).

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

10.8. 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.

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

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

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

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

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

10.11.3. Advises command program managers of required EMSEC countermeasures.

10.12. Ensures compliance with this instruction is accomplished at each command installation by performing annual command Information Assurance Assessment and

Assistance Program assessments according to AFI 33-230, *Information Assurance Assessment and Assistance Program (IAAP)* (will become AFSSI 8560).

11. Host Air Force Wing.

11.1. Establishes 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. When formal agreements allow tenant units to manage their own EMSEC program, ensure a copy of this agreement is retained by the installation EMSEC manager and a copy is provided to the MAJCOM IA office. Appoint an installation EMSEC manager and provide a copy of the appointment letter to the MAJCOM IA office.

11.1.1. Provides IA support for non-Air Force units upon request. Tenant units must follow Air Force regulations while on Air Force installations.

11.1.2. Provides IA support for geographically separated units. Any unit not on an Air Force installation may request support from the nearest IA office. Units will provide funding for this support.

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

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

12. Wing Information Assurance (IA) Office.

12.1. The installation EMSEC Manager is the focal point for all EMSEC requirements and is responsible for management of the installation EMSEC program.

12.2. 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 17).

★12.3. Conducts EMSEC assessments and makes EMSEC countermeasures reviews when required (see paragraph 18).

★12.4. Sends countermeasures review to HQ AFCA/EVPI AF-CTTA according to paragraph 7.5 of AFSSI 7702, *Emission Security Countermeasures Reviews*.

★12.5. Receives validations and sends copy of validated countermeasures to the user.

12.6. Makes EMSEC inspections to determine compliance with EMSEC requirements (see paragraph 21).

12.7. Certifies the information system as meeting EMSEC requirements (see paragraph 22).

12.8. Makes reassessments as required (see paragraph 24).

★12.9. Implements ESIMs and maintains a file of all current EMSEC assessments and countermeasures reviews.

12.10. Ensures the EMSEC Manager and all individuals responsible for EMSEC in the wing IA office receive EMSEC Manager training at Keesler AFB MS.

12.11. 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).

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

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

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

12.15. 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.

12.16. Reviews and approves required countermeasures for contractor facilities supporting wing contracts. Provide a copy to the MAJCOM IA office for concurrence/nonconcurrence.

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

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

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

13. Program Managers.

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

13.1.1. Make sure EMSEC requirements are in the CDD, PMDs, etc.

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

14. Air Force Information Systems Users.

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

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

14.3. Implement required countermeasures.

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

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

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

★14.6.1. Initiate requests for temporary and permanent waivers (see paragraph 26) and EMSEC tests (see AFSSI 7702) when needed.

15. Special Category (SPECAT) Facilities. Facilities that process SPECAT classified information are administered outside the normal chain of command. SPECAT EMSEC management offices are:

15.1. The Office of the Secretary of the Air Force (SAF/AQ). 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 10).

15.2. Defense Intelligence Agency (DIA/DAC-2A2). Provides EMSEC guidance and fulfills the responsibilities of the MAJCOM IA office for all DIA accredited SCIF (see paragraph 10).

15.3. HQ AF ISR Agency. Provides EMSEC guidance and fulfills the responsibilities of the MAJCOM IA office for all National Security Agency accredited SCIFs under Air Force control (see paragraph 10).

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

Section C - Policy

★**16. The Emission Security (EMSEC) 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 33-210, *Air Force Certification and Accreditation [C&A] Program [AFCAP]*). 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. Paragraphs 16.1 through 16.7 show the major steps and where they fit into the C&A process.

16.1. 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.

16.2. The wing IA office determines required IA countermeasures and makes the EMSEC assessments to determine the need for EMSEC countermeasures (see paragraph 17). 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 18). This is the EMSEC portion of determining the security policy for the C&A of the information system.

16.3. The selection of EMSEC countermeasures is validated by the Air Force CTTA (see paragraph 19).

16.4. The required countermeasures are given to the user for application or implementation (see paragraph 20).

16.5. The wing IA office inspects the application of countermeasures for correctness and effectiveness (see paragraph 21). The inspection is made during the security test and evaluation task of the C&A.

16.6. The wing IA office certifies the information system meets EMSEC requirements as part of the certification phase of the C&A (see paragraph 22).

16.7. Processing classified information without complying with the requirements in paragraphs 16.1 through 16.7 is a reportable security incident under AFI 31-401, *Information Security Program Management*, except as allowed for by waiver in paragraph 25.

17. Emission Security (EMSEC) 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.

★17.1. The user/owner determines if the information system will process classified information.

★17.2. If the information system will process classified information, the user must contact the wing IA office.

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

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

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

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

17.3. All IA offices:

17.3.1. Use AFMAN 33-214 Volume 1 (will become AFSSI 7701) to determine required IA countermeasures and make the EMSEC assessments.

17.3.2. Document the IA countermeasures and the EMSEC assessments on AF Form 4170, *Emission Security Assessments/Emission Security Countermeasures Reviews*, according to AFMAN 33-214 Volume 1 (will become AFSSI 7701).

★17.3.3. Verify the basic assessment data (equipment, location, and classification level) annually. Document this as a note, dated and signed in block 6 of the AF Form 4170.

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

★18.1. If the EMSEC assessments determine the need for EMSEC countermeasures, make the appropriate countermeasures reviews according to AFSSI 7702.

★18.2. Document the EMSEC countermeasure reviews on AF Form 4170 according to AFSSI 7702. Use the same form used for the EMSEC assessments.

★**19. 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 AFSSI 7702.

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

21. Emission Security (EMSEC) 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 24).

★**22. Emission Security (EMSEC) Certification.** As a part of the C&A process, the wing IA office certifies that all required EMSEC countermeasures are in place after the EMSEC inspection. Certify the information system as meeting EMSEC requirements of AF Form 4170 according to AFSSI 7702. Recertify during reassessments (see paragraph 24). Document the recertification by dating and signing the AF Form 4170 in or near the certification block of the AF Form 4170. An EMSEC certification memorandum will be provided to the unit according to AFSSI 7702 and a copy will be retained with the AF Form 4170 by the EMSEC Manager. Maintain a copy of the EMSEC certification memorandum with the AF Form 4170 according to AFSSI 7702.

23. Maintaining Emission Security (EMSEC) 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.

★**24. Reassessing Requirements.** Conduct EMSEC reassessments every three years. Reassess when required by a (COMPUSEC) risk analysis (at least every 3 years), the EMSEC threat changes, or when the classification level of the information changes. Make a reassessment by reviewing and confirming the documented information. A new AF Form 4170 is not required 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 becomes illegible, reaccomplish the form. Document the reassessments by dating and signing the AF Form 4170 in or near the authentication and acknowledgement block of the AF Form 4170. If no changes are required at reassessment, initial and date the AF Form 4170 and advise the AF-CTTA by E-mail, specifying the tracking number. This type of reassessment is allowed only once per tracking number. If changes are required, use the template for a new AF Form 4170 and submit with a new number, noting in Block 5 that the new submission supersedes the old tracking number.

★**25. Emission Security Information Messages (ESIM).** ESIMs are issued by the AF- 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 (will become AFSSI 7701) and AFSSI 7702.

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

26.1. 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. Initiate requests for waivers when needed through command EMSEC channels unless otherwise noted in this instruction.

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

26.3. 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 1 year to allow the user to accomplish the mission while they implement or apply required IA or EMSEC countermeasures.

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

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

26.3.1.2. Operation is required for mission accomplishment.

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

26.3.2. 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.

26.3.2.1. For IA and EMSEC information systems countermeasures.

26.3.2.1.1. 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.

26.3.2.1.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC representative to the SPECAT DAA.

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

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

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

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

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

26.3.3. Temporary Waiver Renewals. A 1-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 26.3.2 before the current temporary waiver expires. Temporary waivers are valid as long as the conditions for approval do not change. Moving equipment will invalidate a temporary waiver. After the initial temporary waiver, only two additional renewals are permitted. Waivers will not exceed a cumulative period of 3 years. After 3 years, the information system loses its interim approval to operate.

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

26.4. Permanent Waiver. Only a CTTA may permanently waive a specific 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 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. Moving equipment will invalidate a permanent waiver. Review permanent waivers when making a reassessment of EMSEC requirements. Process requests as follows:

26.4.1. The user initiates the request and sends it to the Wing IA office for review.

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

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

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

27.1. Complete 3 continuous years of EMSEC technical experience, including at least 1 year of experience evaluating vulnerabilities of operational facilities and recommending countermeasures. This requirement cannot be waived.

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

27.3. Complete technical training identified by the CNSS. Only SAF/XCPP may waive technical training requirements.

28. Waivers, Deviations and Exceptions. Requests for exceptions to any of the provisions of this instruction must be submitted through IA channels for approval prior to implementation. All waiver requests for exceptions must be accompanied by complete operational justification.

29. Forms Adopted and Prescribed.

29.1. Adopted Forms. AF Form 847, *Recommendation for Change of Publication*; AF Form 4169**,** *Request For Waiver From Information Assurance Criteria*; and AF Form 4170, *Emission Security Assessments/Emission Security Countermeasures Reviews*.

29.2. Prescribed Forms. No forms are prescribed by this instruction.

★WILLIAM L. SHELTON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

★Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CNSS Policy No. 300, *National Policy on Control of Compromising Emanations*, April 2004

CNSSI 7000, (C) *TEMPEST Countermeasures for Facilities* (U), May 2004

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

DoDD 5100.3, *Support of the Headquarters of Combatant and Subordinate Joint Commands*, November 15, 1999

AFPD 33-2, *Information Assurance*, 19 April 2007

AFI 10-401, *Air Force Operations Planning and Execution*, 7 December 2006

AFI 31-401, *Information Security Program Management.* 1 November 2005

AFI 33-102, *Communications and Information Specialized Publications*, 17 July 2007

★AFI 33-200, *Information Assurance (IA) Management*, 23 December 2008

AFMAN 33-214 Volume 1, (S) *Emission Security Assessments* (U), 15 September 2003 (will become AFSSI 7701)

★AFMAN 33-363, *Management of Records*, 1 March 2008

★AFSSI 7702, *Emission Security Countermeasures Reviews*, 30 January 2008, Incorporating through Change 1, 17 October 2008

AFRIMS RDS, https://afrims.amc.af.mil/rds_series.cfm

Acronyms and Abbreviations

AF—Air Force (used on forms only)

AF ISR—Air Force Intelligence, Surveillance, and Reconnaissance

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

ANG—Air National Guard

C&A—Certification and Accreditation

CDD—Capability Development Document

CNSS—Committee on National Security Systems

CNSSI—Committee on National Security Systems Instruction

COMSEC—Communications Security

COMPUSEC—Computer Security

CTTA—Certified TEMPEST Technical Authority

DAA—Designated Approval Authority

DIA—Defense Intelligence Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

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

MAJCOM—Major Command

NSTISSAM—National Security Telecommunications and Information Systems Security Advisory Memorandum

PMD—Program Management Directive

PSA—Project Support Agreement

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SPECAT—Special Category

Terms

Accreditation--Formal declaration by the 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.

Certified TEMPEST Technical Authority (CTTA)--An experienced, technically qualified government employee who has met established certification requirements according to National Security Telecommunications and Information Systems Security Committee-approved criteria and is appointed by a United States Government department or agency to fulfill CTTA responsibilities.

Collateral Information--All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., SCI) 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.

Emission Security (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.

Emission Security (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 U/FOUO in Committee on National Security Systems Instruction (CNSSI) 7000, (C) *TEMPEST Countermeasures for Facilities* (U).

★**Special Category (SPECAT)—**The definition is FOUO. See CNSSI 7000 (C) TEMPEST Countermeasures for Facilities (U)

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

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*, Level I; or TEMPEST specifications as determined by the department or agency concerned.

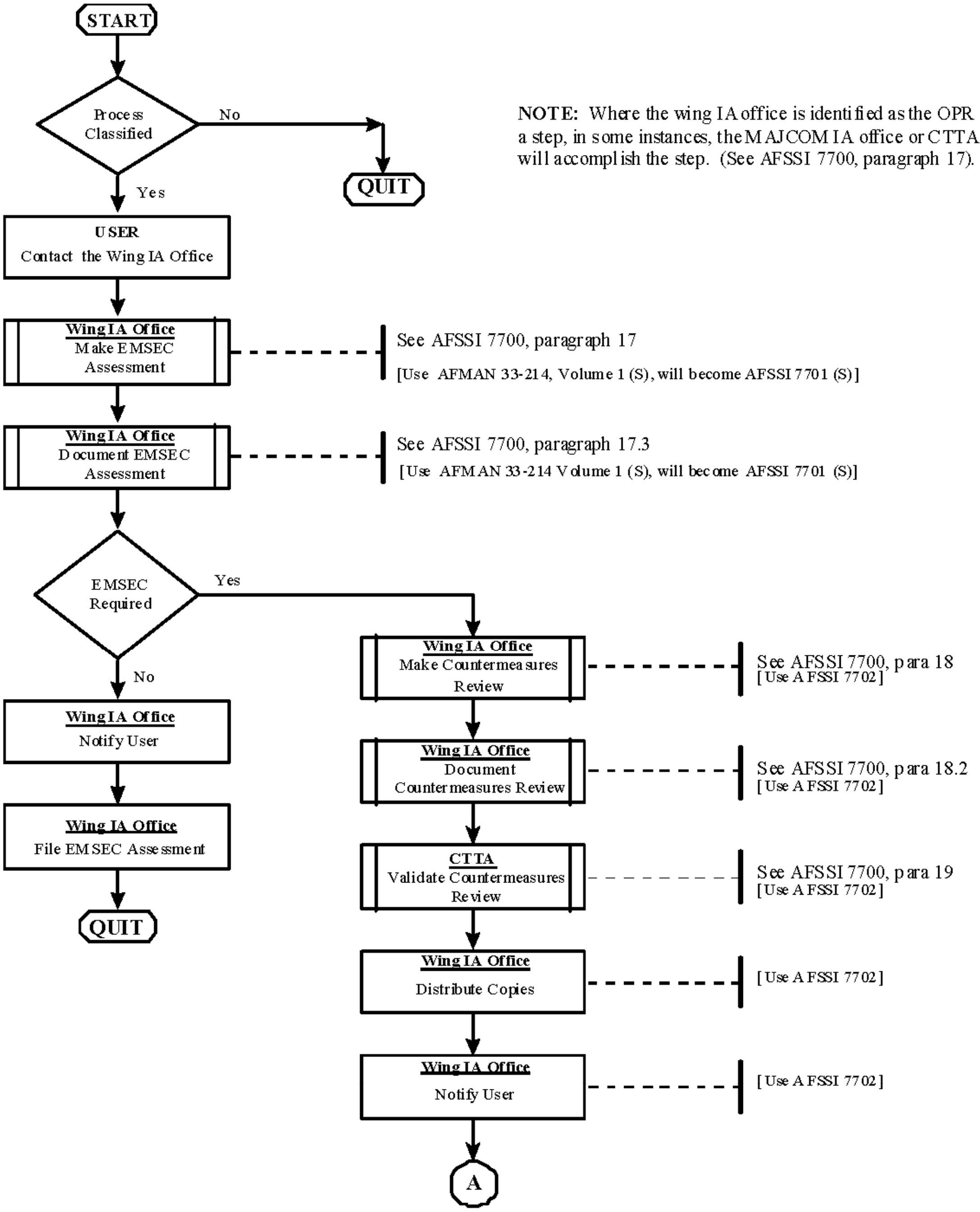
★Attachment 2

THE EMISSION SECURITY (EMSEC) FLOW CHART

A2.1. Use the flowcharts in Figures A2.1 and 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.

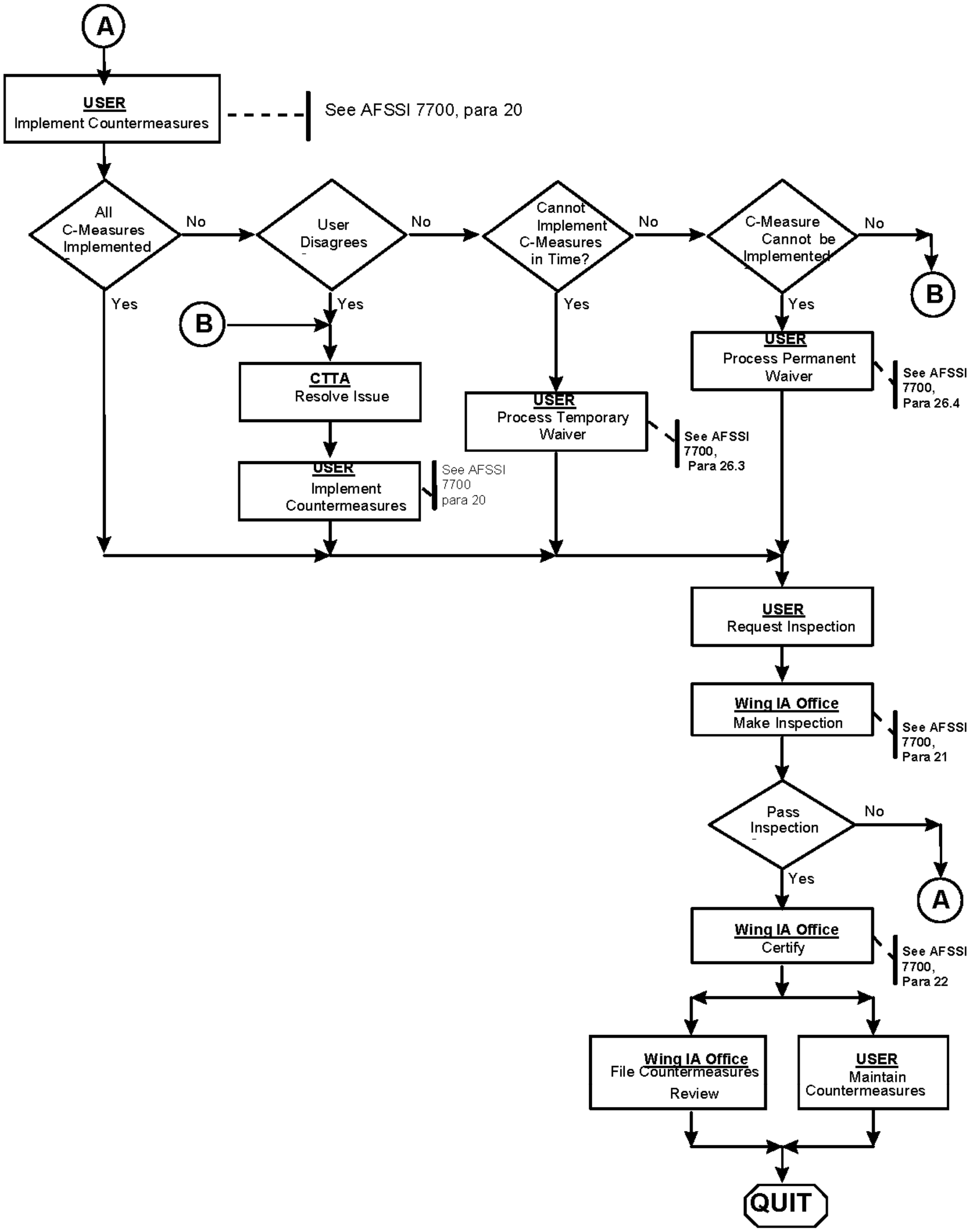
★Figure A2.1. The Emission Security (EMSEC) Flowchart.

Figure A2.1. The Emission Security Flowchart.



NOTE: Where the wing IA office is identified as the OPR for a step, in some instances, the MAJCOM IA office or CTTA will accomplish the step. (See AFSSI 7700, paragraph 17).

Figure A2.2. The Emission Security Flowchart Continued.



Attachment 3

PROCEDURES FOR REQUESTING A TEMPORARY WAIVER FROM INFORMATION ASSURANCE (IA) 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 1 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 sending 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 (SPECAT) 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 sending 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 (IA) 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 sending 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 (SPECAT) 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 sending5 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.