BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-203

1 MAY 1998

Communications and Information

EMISSION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFCA/GCIS (Dwight H. Bohl)
Certified by: HQ USAF/SCXX (Lt Col Webb)
Supersedes AFI 33-203, 1 January 1997.
Pages: 26
Distribution: F

This Air Force instruction (AFI) implements the emission security (EMSEC) portion of Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes Air Force EMSEC requirements for information protection (IP). It interfaces with Air Force Systems Security Instruction (AFSSI) 4100, (C) *Communications Security Program* (U) (will convert to AFI 33-201), AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program* (will convert to AFI 33-202), AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems* (will convert to AFI 33-202), and AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*. We encourage you to use extracts. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5233, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234, and Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNI), 1250 Air Force Pentagon, Washington DC 20330-1250. The Glossary of References and Supporting Information is at **Attachment 1**.

SUMMARY OF REVISIONS

This document was substantially revised and must be completely reviewed. This revision was substantially rewritten to change the emphasis for EMSEC from a stand-alone program to an integral part of IP. It deletes references to acquisition (paragraph 2), and implements the EMSEC certification part of the certification and accreditation process (paragraph 9). It also clarifies application of the instruction to those contractors who contract to perform Air Force functions (paragraph 2). It clarifies the three EMSEC assessments (paragraph 2.1.1) and three EMSEC countermeasures reviews (paragraph 5), and the process to authenticate them (paragraphs 4.3.2, 5.3, 6, 8, and 9). It adds the basic steps for validating EMSEC countermeasures reviews (paragraph 6), adds the requirement for the user to notify the wing IP office to make the EMSEC inspection (paragraph 4.2), and removes the annual requirement for EMSEC inspections (paragraph 8). It provides instructions for the EMSEC certification (paragraph 9) and removes the instruction for a reassessment during an annual inspection (paragraph 8). It makes one level of authority for approving temporary waivers (paragraph 11.2.2.1.1). It replaces reference to the term

"command, control, communications, and computer (C4)" with "information systems". It deletes Air Force Communications Security (AFCOMSEC) Form 7001, **Emission Security Assessment/Emission Security Countermeasures Review**, from being prescribed by this publication (it is now prescribed by AFSSI 7010, [S] *The Emission Security Assessment [U]*).

Section A—The Emission Security Program.

1. Introduction. The Air Force EMSEC process has experienced many changes. Although these changes were attempts to meet the variances of a dynamic world, they require security protection measures far beyond the needs of the average user. In the past, EMSEC tended to stand alone; however, IP now requires a more balanced approach not only to the control of compromising emanations, NONSTOP, and HIJACK, but to communications security (COMSEC); COMPUSEC; and SATE as well. The prime objective of EMSEC is to identify requirements from the standpoint of IP risk management principles and provide the appropriate protection at the least possible, or no, cost. Key to this process is a partnership between the wing IP office and the user. The wing IP office assesses the need for EMSEC as part of IP; determines the required countermeasures; advises commanders of vulnerabilities, threats, and risks; and recommends a practical and feasible course of action to the wing commander. The user applies identified countermeasures.

2. Emission Security Requirements. Air Force organizations and contractors doing business as the Air Force, whether procuring or using systems to process classified national security information, must apply EMSEC proportional to the threat of exploitation.

2.1. They must consider the potential damage to national security if classified national security information is compromised, and:

2.1.1. Assess the need for EMSEC for each aspect (control of compromising emanations, NONSTOP, and HIJACK) and determine the specific countermeasures before beginning architectural engineering and facility design, procuring systems, or beginning engineering and installation.

2.1.2. Implement or apply required countermeasures before using systems to process classified national security information.

2.1.3. Operate and maintain systems to preserve the integrity of required countermeasures.

2.2. Processing classified national security information without complying with the above requirements is a reportable security incident under AFI 31-401, *Managing the Information Security Program*, except as allowed for by waiver in paragraph 11.

3. Emission Security Process. Assess equipment and facilities to determine the need for EMSEC (control of compromising emanations, NONSTOP, and HIJACK); determine, validate, and implement or apply the required countermeasures; and periodically reassess EMSEC requirements. The following paragraphs further define this process (see **Attachment 2**).

4. Emission Security Assessments. This process determines the need for EMSEC for a system that processes classified national security information.

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

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

4.2.1. The wing IP office makes the EMSEC assessment for wing-level systems and programs.

4.2.2. The major command (MAJCOM) IP office makes the EMSEC assessment for MAJCOM-level programs.

4.2.3. The lead MAJCOM IP office, or the certified TEMPEST technical authority (CTTA), makes the EMSEC assessments for Air Force-level programs.

4.2.4. For Special Category (SPECAT) information, the CTTA makes the EMSEC assessments.

4.3. All IP offices:

4.3.1. Use AFSSI 7010 to make the assessments.

4.3.2. Document the EMSEC assessment on AFCOMSEC Form 7001 according to AFSSI 7010.

5. Emission Security Countermeasures Reviews . This process determines the needed control of compromising emanations, NONSTOP, and HIJACK countermeasures for a system that processes classified national security information.

5.1. If the EMSEC assessment determined the need for the control of compromising emanations, NONSTOP, or HIJACK, make the appropriate countermeasures review. Use Air Force Systems Security Memorandum (AFSSM) 7011, *The Emission Security Countermeasures Review* to make each review.

5.2. The same IP office that made the EMSEC assessments makes the EMSEC countermeasures review.

5.3. Whenever possible, document the EMSEC countermeasures reviews on the same AFCOMSEC Form 7001 used for the EMSEC assessments. Where this is not possible, complete an additional AFCOMSEC Form 7001 for the countermeasures review with an appropriate reference to the associated assessment.

6. Validation Requirements. The CTTA must validate the EMSEC countermeasures review because of the costs involved in applying countermeasures to some facilities and the cost of some countermeasures. Validate EMSEC countermeasures reviews according to AFSSM 7011. Whenever possible, document the validation on the same AFCOMSEC Form 7001 used for the EMSEC countermeasures review. Where this is not possible, complete an additional AFCOMSEC Form 7001 for the validation with an appropriate reference to the associated assessment and countermeasures review.

7. Applying Countermeasures. The user applies, implements, and maintains the required countermeasures identified by the EMSEC countermeasures review. Notify the wing IP office when completed.

8. Emission Security Inspection. Upon notification from the user, the wing IP office makes an EMSEC inspection to make sure the required EMSEC countermeasures are effectively applied or implemented. The EMSEC countermeasures review is 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 national security information.

9. Emission Security Certification. As a part of the certification and accreditation process, the wing IP office certifies all required EMSEC countermeasures are in place after the EMSEC inspection. Certify the system as meeting EMSEC requirements according to AFSSM 7011. Whenever possible, document the EMSEC certification on the same AFCOMSEC Form 7001 used for the EMSEC countermeasures review.

Where this is not possible, complete an additional AFCOMSEC Form 7001 for the certification with an appropriate reference to the associated assessment, countermeasures review, and validation.

10. Reassessing Requirements. Reassess EMSEC requirements when required by a COMPUSEC risk analysis, the threat changes, or when the classification level of the information changes. Make a reassessment by reviewing and confirming the information on the AFCOMSEC Form 7001 is still valid. You do not need a new AFCOMSEC Form 7001 for changes such as equipment, office, room, or building changes, that do not change the outcome of the EMSEC assessment or countermeasures review. Make pen and ink changes instead. If the form gets too messy, re-accomplish the form.

11. Waivers. There are two kinds of EMSEC waivers: temporary and permanent.

11.1. AFCOMSEC Form 3331, **Request for Waiver From Information Protection Criteria.** Use this form to document and request either a temporary (see **Attachment 3**) or permanent waiver (see **Attachment 4**). Attach a copy of the EMSEC countermeasures review.

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

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

11.2.1.1. All required EMSEC countermeasures were not installed or applied during installation.

11.2.1.2. Operation is required for mission accomplishment.

11.2.1.3. The user cannot install all required EMSEC countermeasures before system turn-on.

11.2.2. Processing a Temporary Waiver. The user originates the request for a temporary waiver, then sends it to the wing IP office for coordination, and approval or disapproval by the appropriate authority.

11.2.2.1. The control of compromising emanations.

11.2.2.1.1. For collateral information, the approval authority for the temporary waiver is the designated approving authority (DAA).

11.2.2.1.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC person to the SPECAT DAA.

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

11.2.2.2. NONSTOP and HIJACK. The CTTA approves all NONSTOP and HIJACK temporary waivers. **NOTE:** The terms NONSTOP and HIJACK have classified definitions (see AFSSI 7010).

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

11.2.2.2.2. For SPECAT information, process the temporary waiver through the SPECAT EMSEC person to HQ AFCA/GCIS.

11.2.2.2.3. For GCCS information, process the temporary waiver through the MAJCOM

IP office to HQ AFCA/GCIS.

11.2.3. Temporary Waiver Renewals. A temporary waiver is renewable for one year only if the user is making an active effort to correct the problem; otherwise do not renew it. Process a renewal according to paragraph 11.2.2 before the current temporary waiver expires. Only two renewals are permitted.

11.2.4. Temporary Waiver Cancellations. Cancel the temporary waiver after applying the required EMSEC countermeasures (see **Attachment 3** for instructions).

11.2.5. Temporary Waiver Copies. Forward a copy of all temporary waivers, including renewals and cancellations, to the MAJCOM IP office or SPECAT EMSEC person and HQ AFCA/GCIS.

11.3. Permanent Waiver. Only a CTTA may waive a specific EMSEC countermeasure. Such things as an extremely low volume of classified national security 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 IP 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. Process requests as follows:

11.3.1. The user initiates the request and forwards the request to the wing IP office for review.

11.3.2. The wing IP office reviews the request for validity and, if valid, forwards the request to the MAJCOM IP office or SPECAT EMSEC person for review.

11.3.3. The MAJCOM IP office or SPECAT EMSEC person reviews the request and, if valid, forwards the request, along with appropriate supportive comments, to HQ AFCA/GCIS.

Section B—Responsibilities.

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

12.1. HQ AFCIC/SYNI. Responsible for the EMSEC program according to AFPD 33-2. It 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.

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

12.2.1. Air Force Civil Engineer Support Agency (HQ AFCESA/CESE). The office of primary responsibility (OPR) for guidance, information, standards, and requirements for design and construction of facilities containing RFI and EMI shielding. *The USAF Handbook for the Design and Construction of HEMP/TEMPEST Shields in Facilities* is the HQ AFCESA/CESE document that provides this guidance, information, standards, and requirements.

12.3. HQ AFCA:

12.3.1. Manages the Air Force EMSEC requirements.

12.3.2. Is assigned CTTA responsibility (see paragraph 13).

12.3.3. Distributes guidance on the domestic and foreign technical threat environment as provided by the National Security Agency (NSA).

12.3.4. Tasks all Air Force EMSEC testing.

12.3.5. Advises Headquarters Air Education and Training Command (HQ AETC) on EMSEC curriculum.

12.3.6. Provides Air Force EMSEC requirements and guidance for Air Force systems.

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

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

12.4. Headquarters Air Intelligence Agency (HQ AIA). Through the Air Force Information Warfare Center (AFIWC):

12.4.1. Provides NONSTOP and HIJACK testing and a quick reaction capability to support emergency testing of facilities.

12.4.2. Provides a capability for limited testing of high value Air Force systems such as special air mission aircraft and strategic systems such as F-117, B-2, or special access required programs.

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

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

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

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

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

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

12.5. MAJCOMs (include those field operating agencies [FOA] and direct reporting units [DRU] who have established IP offices [see paragraph 12.7.1.1]):

12.5.1. Establish EMSEC as a part of IP in the MAJCOM IP office. Include those Air National Guard (ANG) and United States Air Force Reserve units gained by the MAJCOM upon activation.

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

12.5.3. Include EMSEC requirements when preparing the COMSEC appendix to the communications annex of operations plans according to Air Force Manual (AFMAN) 10-401, *Operation Plan and Concept Plan Development and Implementation.*

12.5.4. Implement and maintain required countermeasures for systems that process classified national security information.

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

12.5.6. Ensure inspection of all facilities that have EMSEC requirements (see paragraph 8).

12.6. MAJCOM IP Office:

12.6.1. The OPR for MAJCOM EMSEC requirements.

12.6.2. Makes sure the person responsible for EMSEC in the IP office receives EMSEC training.

12.6.3. Provides EMSEC guidance and assistance to the command staff and subordinate wing IP offices.

12.6.4. Assists wing IP offices by making EMSEC assessments, countermeasures reviews, and EMSEC inspections when requested.

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

12.6.6. 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.

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

12.6.8. Reviews MAJCOM programming and requirements documents that call for the processing of classified national security information.

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

12.6.9.1. Reviews all project support agreement (PSA) changes and project packages for facilities that process classified national security information.

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

12.6.9.3. Advises command program managers of required EMSEC countermeasures.

12.7. Host Air Force Wings:

12.7.1. Establish EMSEC as a part of IP in the host wing IP office. The wing IP 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.

12.7.1.1. A wing IP office may support non-Air Force units if the unit's own service does not, and the unit requests support.

12.7.2. Include a wing IP office representative in planning meetings for new equipment procurement, installation, or reconfiguration of existing facilities that process classified national security information.

12.7.3. Assist the wing IP office to determine EMSEC requirements and, when required, cost estimates of required countermeasures during initial meetings for new facility construction or upgrade projects.

12.8. Wing IP Office:

12.8.1. Manages wing EMSEC requirements.

12.8.2. Makes EMSEC assessments of all systems that process classified national security information on the base, including those of tenant organizations, unless there are other formal agreements.

12.8.3. Makes EMSEC countermeasures reviews when required.

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

12.8.5. Forwards a copy of all EMSEC countermeasures reviews according to AFSSM 7011.

12.8.6. Ensures the person responsible for EMSEC in the wing IP office receives EMSEC training.

12.8.7. Conducts and documents required EMSEC inspections.

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

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

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

12.8.11. Provides Headquarters 38 Engineering Installation Wing with countermeasure requirements for information systems before engineering and installation begins.

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

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

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

12.8.15. Reviews all PSAs, PSA changes, and project packages for facilities that will process classified national security information, to include applicable EMSEC requirements.

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

12.8.17. Coordinates on AF Form 1261, **Command, Control, Communications and Computer Systems Acceptance Certificate**, before the user processes any classified national security information.

12.9. HQ AETC. In addition to the responsibilities in paragraph 12.5, HQ AETC:

12.9.1. Trains or provides training to installers, operators, and maintenance technicians of systems that process classified national security information.

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

12.9.3. Works with HQ AFCA/GCIS to make sure EMSEC portions of curriculums are current and meet Air Force needs.

12.10. Headquarters Air Force Materiel Command (HQ AFMC). In addition to the responsibilities in paragraph 12.5, HQ AFMC:

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

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

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

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

12.10.5. 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 HQ AFIWC/EAC.

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

12.10.7. Installs equipment and systems according to EMSEC standards.

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

12.10.9. Coordinates exchange of engineering and installation EMSEC information with HQ AFCA/GCIS.

12.10.10. Performs shielding effectiveness testing when requested.

12.10.11. 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.

12.11. Program Managers. Responsible for early coordination with MAJCOM IP offices, SPECAT EMSEC persons, and wing IP offices to:

12.11.1. Make sure EMSEC requirements are in MNSs, ORDs, etc.

12.11.2. Establish EMSEC requirements at the system's planned locations.

12.12. Air Force Information Systems Users:

12.12.1. Contact the wing IP office (FOA or DRU IP office for those FOAs and DRUs managing their own EMSEC requirements) for assistance when the need to process classified national security information arises.

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

12.12.3. Implement required countermeasures.

12.12.4. Request the wing IP office perform an EMSEC inspection, after installation, but before operation, if required.

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

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

12.12.7. Initiate requests for temporary and permanent waivers (see paragraph 11) and EMSEC tests (see AFSSM 7011), when needed.

12.13. SPECAT Facilities. Facilities that process SPECAT classified national security information are administered outside the normal chain of command. SPECAT EMSEC persons are:

12.13.1. Defense Intelligence Agency (DIA/DAC-2A). The office where the Sensitive Compartmented Information (SCI) EMSEC person is located. For all DIA accredited SCI facilities (SCIF), this office fulfills the responsibilities of the MAJCOM IP office identified in paragraph 12.5.

12.13.2. HQ AIA/SOXS. The office where the EMSEC person is located for facilities accredited by NSA. For all NSA accredited SCIFs, this office fulfills the responsibilities of the MAJCOM IP office identified in paragraph 12.5.

12.13.3. Office of the Secretary of the Air Force (SAF/AQ-PJ). The office where the EMSEC person is located for special access required and special access programs. For all special access required and special access program accredited facilities, this office fulfills the responsibilities of the MAJCOM IP office identified in paragraph 12.5.

12.13.4. For all other SPECAT facilities, contact HQ AFCA/GCIS for guidance.

Section C—Qualifications and Classification.

13. Certified TEMPEST Technical Authority. A CTTA is an experienced, technically qualified government employee who meets established certification requirements according to National Security Telecommunications and Information Systems Security Committee-approved criteria and appointed by HQ AFCIC/SYNI 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:

13.1. Complete three continuous years of EMSEC technical experience, including at least one year of experience evaluating vulnerabilities of operational facilities and recommending countermeasures.

13.2. Complete mandatory training on the technical threat.

13.3. Complete technical training identified by the National Manager for National Security Telecommunications and Automated Information Systems Security. HQ AFCIC/SYNI may waive technical training requirements.

14. Classification Guidance. AFMAN 33-272, (S*) Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information* (U), is the classification guide for EMSEC matters.

15. Form Prescribed:

15.1. AFCOMSEC Form 3331, **Request for Waiver From Information Protection Criteria**.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, *Information Protection*

AFI 31-401, *Managing the Information Security Program*

AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*

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

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

AFMAN 33-272, (S) *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U)*

AFSSI 4100, (C) *Communications Security Program (U)* (will be replaced by AFI 33-201)

AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program* (will be replaced by AFI 33-202)

AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems* (will be replaced by AFI 33-202)

AFSSI 7010, (S) *The Emission Security Assessment (U)*

AFSSM 7011, *The Emission Security Countermeasures Review*

Executive Order 12958, *Classified National Security Information*, April 17, 1995

The USAF Handbook for the Design and Construction of HEMP/TEMPEST Shields in Facilities

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFCA—Air Force Communications Agency

AFCESA—Air Force Civil Engineer Support Agency

AFCIC—Air Force Communications and Information Center

AFCOMSEC—Air Force Communications Security (used on forms)

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

AIA—Air Intelligence Agency

ANG—Air National Guard

C4—Command, Control, Communications, and Computer (term replaced by “Information Systems”)

COMSEC—Communications Security

COMPUSEC—Computer Security

CTTA—Certified TEMPEST Technical Authority

DAA—Designated Approving Authority

DIA—Defense Intelligence Agency

DoD—Department of Defense

DRU—Direct Reporting Unit

EMI—Electromagnetic Interference

EMSEC—Emission Security

FOA—Field Operating Agency

GCCS—Global Command and Control System

IP—Information Protection

MAJCOM—Major Command

MNS—Mission Need Statement

NSA—National Security Agency

OPR—Office of Primary Responsibility

ORD—Operational Requirements Document

PSA—Project Support Agreement

RFI—Radio Frequency Interference

SATE—Security Awareness, Training, and Education

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facility

SPECAT—Special Category

USAF—United States Air Force

Terms

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 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., 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 automated information system.

Countermeasures Review—A technical evaluation of a facility to identify the inspectable space, the required countermeasures, and the most cost-effective way to apply required countermeasures.

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

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

Emission Security Assessment—An evaluation of a facility to determine the need for emission security.

Emission Security Countermeasures Review—A review of a facility to determine needed countermeasures.

Equipment Radiation TEMPEST Zone—A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

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 which contains classified national security information-processing equipment.

Hazard—A measure of both the existence and the compromising nature of an emanation. Hazards exist if, and only if compromising emanations are detectable beyond the inspectable space.

HIJACK—The definition of HIJACK is classified (see AFSSI 7010).

Information Systems—(DoD) The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information.

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.

National Security Information—Information that has been determined, pursuant to Executive Order 12958, *Classified National Security Information*, April 17, 1995, or any predecessor order, to require protection against unauthorized disclosure, and is so designated.

NONSTOP—The definition of NONSTOP is classified (see AFSSI 7010).

RED and BLACK Concept—Separation of electrical and electronic circuits, components, equipment,

and systems that handle classified plain text (RED) information in electrical signal form from those which handle unclassified (BLACK) information in the same form.

Service Cryptologic Element—A term used to designate separately or together those elements of the United States Army, United States Navy, and United States Air Force that perform cryptologic functions.

Special Category (SPECAT) Information—The definition of SPECAT is classified (see AFSSI 7010).

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—Systems or equipment that were certified within the requirements of the effective edition of NSTISSAM TEMPEST/1-92, 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.

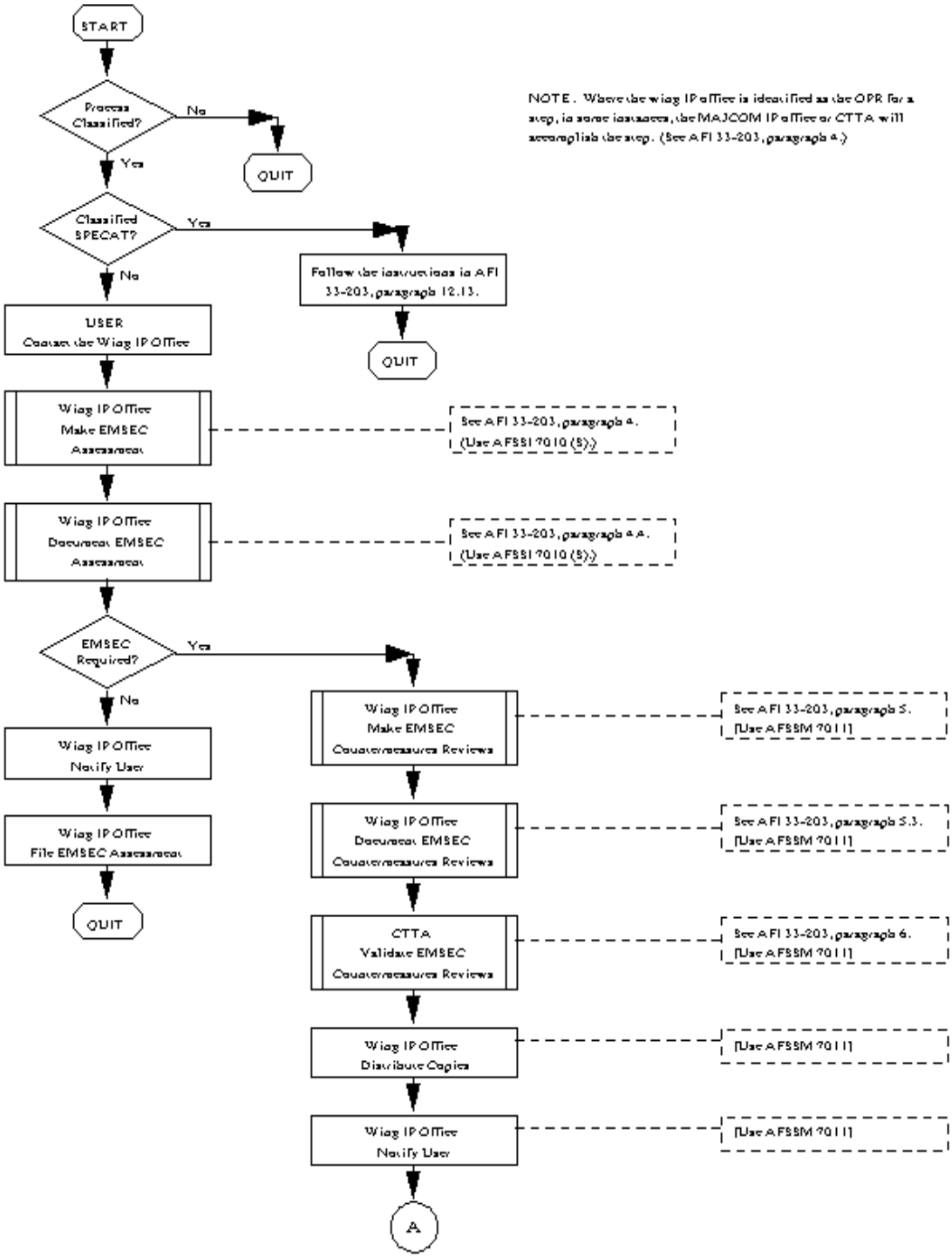
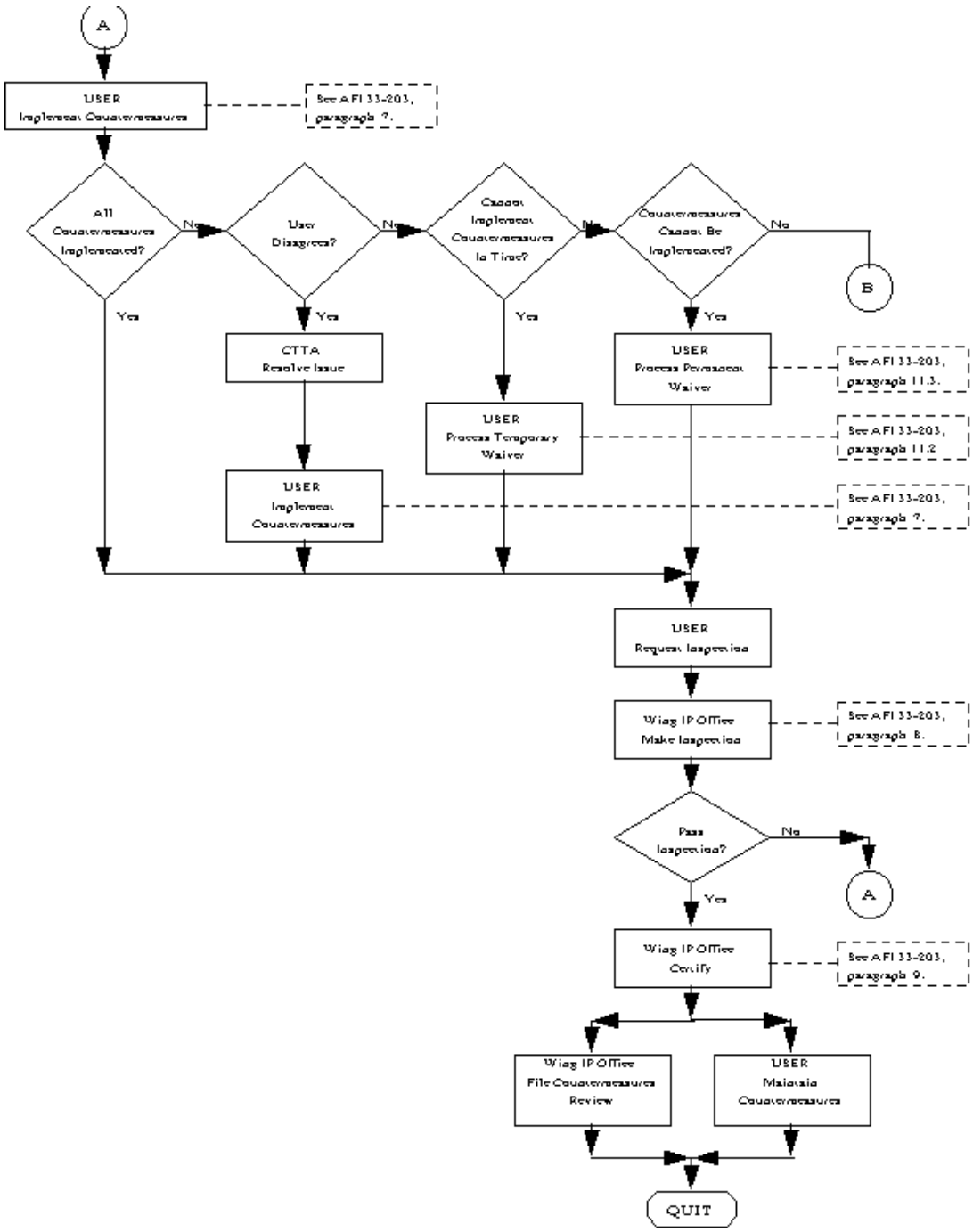


Figure A2.2. The Emission Security Flowchart Continued.



Attachment 3

PROCEDURES FOR COMPLETING AFCOMSEC FORM 3331 FOR A TEMPORARY WAIVER

A3.1. Temporary Waiver. This attachment provides guidance for completing AFCOMSEC Form 3331 for a temporary waiver. Due to the limited space on the AFCOMSEC Form 3331, attach additional information as required.

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

A3.2.1. Block 1: The wing IP office numbers the initial temporary waiver using the following format: MAJCOM, base, requesting unit, last two digits of year, minimum two digit temporary waiver number with a "T". Use the original temporary waiver number for renewals. **EXAMPLES:** ACC-Langley-1776ABW-95-01T, AFMC-Edwards-1925CS-95-104T.

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 IP 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 countermeasures 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 national security information without meeting all the required countermeasures. For example, what is the mission impact of not processing? Why can't you apply the countermeasures before system turn-on? Attach a copy of the EMSEC countermeasures review, AFCOMSEC Form 7001.

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, "countermeasures applied" or "equipment no longer used to process classified national security 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 wing IP office is mandatory. It is the last review before forwarding the request to the DAA. You cannot have more than two reviews.

A3.2.16. First Reviewing Official.

A3.2.16.1. TO: The wing IP office.

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

A3.2.17.1. TO: The DAA.

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

A3.2.17.3. Block 16 or 22: As necessary within the wing IP 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 IP office and the SPECAT EMSEC person is mandatory and is the last review before forwarding the request to the approving authority. If you need reviews in addition to the wing IP office and SPECAT EMSEC person, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.

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

A3.3.4.1. TO: The next level for review or the wing IP 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 IP Office’s Review.

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

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

A3.3.5.3. Block 16: As necessary within the wing IP 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 Person’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 COMPLETING AFCOMSEC FORM 3331 FOR A PERMANENT WAIVER

A4.1. Permanent Waiver. This attachment provides guidance for completing the AFCOMSEC Form 3331 for a permanent waiver. Due to the limited space on the AFCOMSEC Form 3331, attach additional information as required.

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

A4.2.1. Block 1: The wing IP office numbers the initial permanent waiver using the following format: MAJCOM, base, requesting unit, last two digits of year, minimum two digit permanent waiver number with a "P". EXAMPLES: ACC-Langley-1776ABW-95-01P, AFMC-Edwards-1925CS-95-104P.

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

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

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

A4.2.5. Block 3: Check "permanent."

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; one countermeasure to a request for a permanent waiver.

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 national security information without applying the required countermeasure. For example, why can't the required countermeasure be applied? Attach a copy of the countermeasures review, AFCOMSEC Form 7001.

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 IP 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 IP offices, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.

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

A4.2.15.1. TO: The next level for review or the wing IP 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 IP Office’s Review.

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

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

A4.2.16.3. Block 16: As necessary within the wing IP 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 IP Office’s Review.

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

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

A4.2.17.3. Block 16: As necessary within the MAJCOM IP 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/GCIS.

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 IP 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 IP office and

SPECAT EMSEC person, attach additional AFCOMSEC Forms 3331 using only the reviewing official blocks.

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

A4.3.4.1. TO: The next level for review or the wing IP 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 IP Office's Review.

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

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

A4.3.5.3. Block 16: As necessary within the wing IP 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 Person's Review.

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

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

A4.3.6.3. Block 16: As necessary within the SPECAT EMSEC person'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.