

1 DECEMBER 2003



Communications and Information

INFORMATION ASSURANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: 45 SCS/SCBI (Mrs. Debra Storey)

Certified by: 45 SCS/CC
(Lt Col Albert P. Zelenak, Jr.)

Pages: 15

Distribution: F

This instruction implements guidelines contained in Air Force Policy Directive (AFPD) 33-2, *Information Protection*; Air Force Instruction (AFI) 33-211, *Communications Security (COMSEC) User Requirements*; AFI 33-203, *Emissions Security (EMSEC)*; AFI 33-202, *Computer Security (COMPUSEC)*; AFI 33-204, *Information Assurance (IA) Awareness Program*; and AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, and other applicable IA directives. This instruction applies to all 45th Space Wing (45 SW) and tenant organization personnel, including civilians under contract by organizations that procure, install, operate, and/or maintain telecommunications equipment that processes classified and/or unclassified information on a full or part time basis. By establishing IA policy specifically for use in the wing, it acts as an addendum to other IA instructions and directives. Refer questions on the content of this instruction to the Chief, Wing Information Assurance Office (WIAO), 45 SCS/SCBI, 494-6145 (DSN 854-6145).

1. Wing Information Assurance Office (WIAO).

1.1. **Overview.** The WIAO provides guidance in the development and management of wing COMSEC, EMSEC, COMPUSEC, TMAP and IA Awareness programs. WIAO members implement services for wing users by providing policy, guidance, training and assessments to ensure the highest level of telecommunication security is maintained. These services include COMSEC management and account operations, COMSEC controlling authority responsibilities, EMSEC countermeasures, secure telephone unit/equipment (STU or STE) management, COMPUSEC assessments, TMAP certification, and IA awareness educational material.

1.2. **Tenant Services.** The WIAO also provides tenants with training for the IA security disciplines and guidance from Air Force, Air Force Space Command (AFSPC) and wing IA offices. Tenants comply with their major command IA instructions. If tenants request additional support not included in the Host-Tenant Support Agreement that requires expenditure of manpower or financial resources,

a functional-level memorandum of agreement is required. Wing Plans and Programs (45 SW/XP) is the focal point for wing level agreements.

1.3. Incident Response. The WIAO participates as a member of the Wing Computer Emergency Response Team (45SWCERT). The 45SWCERT focal point is the Network Control Center (NCC), and the wing commander (45 SW/CC) directs and approves all actions. The 45SWCERT responds to IA emergencies (e.g., virus activity, hackers, etc.) involving wing assets.

1.4. Certification and Accreditation (C&A) Tracking.

1.4.1. Certification and Accreditation Tracking System (CATS). The WIAO tracks the accreditation status of all wing systems and updates these statuses in CATS. Each month, notices are sent to the certifier and information system security officer (ISSO) of any system that requires accreditation or has an accreditation due to expire within 90 days.

1.4.2. Base Information System Network Accreditation Verification Procedure. The WIAO accumulates metrics of network accreditation status for communications and information briefings to the DAA. The WIAO generates a monthly connectivity summary report for the NCC to review and take appropriate action. In preparation for the unit information assurance assessment program (IAAP) inspection, the WIAO ensures there is no connectivity without a network service level agreement.

1.5. IA Assessments. The WIAO performs assessments in accordance with AFI 33-230. All deficient items identified in this report must be addressed within 30 days of receipt. Replies must address the specific actions taken to correct and eliminate the basic cause of deficiencies and provide enough detail to permit effective evaluation. The WIAO is the final authority on determining the adequacy of responses and for closing individual deficiencies or reports. Follow-up reporting is required for all findings every 30 days until all findings are resolved. The report remains open until all deficiencies have been resolved.

1.5.1. COMPUSEC, TMAP, and IA Awareness Assessments. The WIAO will annually assess unit TMAP, IA awareness and COMPUSEC programs. IA assessments will be performed annually on all wing units and contractors processing government data in accordance with Air Force guidance. Security programs will be graded using the unit and system checklists and receive a satisfactory or unsatisfactory grade. The unit and system checklists are WIAO checklists that incorporate the applicable portions of the AF Form 4160 checklist. The unit and system checklists used by the WIAO during assessments are located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/CompuSec.htm>). (It is advised that organizations run the WIAO checklist as part of their Inspector General (IG) compliance self-inspections.)

1.5.2. COMSEC Assessments. The WIAO will conduct COMSEC assessments each February and August in conjunction with the inventory of COMSEC holdings. COMSEC sub-accounts will be graded using the Air Force Form 4160 checklist.

1.5.3. EMSEC Assessments. The WIAO reassesses EMSEC requirements when required by a COMPUSEC risk analysis, when the threat changes, or when the classification level of the information changes. Hardware/software modifications and system connectivity changes will also trigger an EMSEC reassessment. In addition, systems will be re-assessed upon expiration of their respective accreditation packages.

1.6. **Communications and Information Steering Group.** Through the C&I Steering Group, the WIAO provides both insight and metrics to 45 SW/CC and senior staff on the security posture of the wing. In accordance with 45 SW/CC guidance, assessment results will be briefed in lieu of forwarding written reports.

1.7. **IA Training Overview.** The WIAO provides oversight and training for all IA security services. An excellent online resource is the WIAO Intranet website (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI>). (For more IA information, refer to **Attachment 2**, "On-line Resources.") WIAO members are available to brief customers at commanders' calls and other such gatherings.

1.8. **Contact and Additional Information.** The WIAO is organizationally located within the 45th Space Communications Squadron (45 SCS) under the Information Systems Flight (45 SCS/SCB). The WIAO (45 SCS/SCBI) E-mail address is <mailto:45SWIAO@patrick.af.mil>. The WIAO Chief, 45 SCS/SCBI, can be contacted at 494-6145 (DSN 854-6145).

2. COMSEC Program.

2.1. **Overview.** The purpose of the COMSEC program is to prescribe procedures including the application of physical security measures for safeguarding, controlling, and destroying COMSEC material (e.g., STU keys, Fortezza cards). COMSEC users will contact the base COMSEC manager, 45 SCS/SCBIJ, to establish a COMSEC sub-account. Users should reference AFI 33-211_AFSPC Supplement 1 for more detailed information and may obtain assistance and guidance from the WIAO for IA requirements.

2.2. **STU Responsible Officer.** Each organizational/unit commander will appoint in writing an individual to be a focal point for unit STU issues when there is no unit COMSEC responsible officer (CRO). If the wing COMSEC manager determines circumstances warrant the CRO and STU responsible officer (SRO) to be a different individual, there will be two different accounts. The actual STU will be procured through base supply channels.

2.3. **Fortezza for Classified.** Each organization issued FFC is required to annually provide proof of FFC accountability. This will be accomplished by verification of the FFC card's serial number when brought to the base communications center (BCC) by the designated cardholder. The designated FFC cardholder will be required to furnish a valid form of photographic identification as part of the verification process.

2.4. **Appointment Letters.** Appointments to SRO and CRO will be made in writing and will be signed by the applicable unit commander. Forward SRO, CRO and other COMSEC-related appointment letters to 45 SCS/SCBIJ. Recommended format for all appointment letters is located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Appointments/Appointments.htm>).

2.5. **Training.** CRO and SRO training is available monthly. Call the COMSEC office for additional information, and a notification E-mail will be sent providing dates and times of training sessions.

2.6. **Contact and Additional Information.** The base COMSEC manager, 45 SCS/SCBIJ, can be contacted at 494-5476 (DSN 854-5476). Customers requiring COMSEC at Cape Canaveral Air Force Station (CCAFS) need to contact the Range Technical Support Contractor, CCAFS COMSEC office at 853-5460 (DSN 467-5460). COMSEC information is located on the 45 SW Intranet (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/ComSec/ComSec.htm>).

3. EMSEC Program.

3.1. **Overview.** The purpose of EMSEC is to deny information contained in radiated signals to the enemy by providing the appropriate protection at the least possible cost during classified processing. EMSEC applies to all government, contractor and tenant units who process classified government information. Users should reference AFI 33-203 or Air Force Manual (AFMAN) 33-214, Volume 2 for more detailed information and may obtain assistance and guidance from the WIAO.

3.2. **EMSEC Accreditation Process.** The using organizations must submit any notifications, replies or requests for EMSEC services in writing or via E-mail. To initiate the EMSEC accreditation process for a system, using organizations must provide lists of all equipment connected to the system, buildings housing the equipment, and floor plans indicating where any and all system equipment will be located for processing the classified national security information.

3.3. Roles and Responsibilities.

3.3.1. The 45 SW/CC will appoint, in writing, a wing EMSEC manager (also referred to as the WEM).

3.3.2. The 45th Space Communications Squadron Commander (45 SCS/CC) will:

3.3.2.1. Ensure the wing EMSEC program is administered in accordance with applicable directives.

3.3.2.2. Review the communications annex of applicable operations plans to ensure EMSEC requirements are included, if needed.

3.3.3. The WEM will:

3.3.3.1. Administer the wing EMSEC program in accordance with applicable directives.

3.3.3.2. Keep a current list of unit EMSEC monitors.

3.3.3.3. Ensure all AF Forms 3215, **Communications-Computer Systems Requirements Documents**, are routed through the appropriate unit EMSEC monitor.

3.3.3.4. Be the focal point for all EMSEC matters, including messages and reports, between MAJCOM and unit EMSEC monitors.

3.3.3.5. Review all AF Forms 3215 that unit EMSEC monitors have identified as being related to information systems that process classified information.

3.3.3.6. Maintain a reference library of EMSEC documents applicable to the wing.

3.3.3.7. Implement an ongoing EMSEC training and education program for all personnel involved in the electronic processing of classified national security information, the procurement of classified equipment, or the correction of EMSEC discrepancies.

3.3.3.8. Ensure that annual EMSEC inspections of all facilities that process classified national security information are performed and documented as required, and that corrective actions are being taken by the appropriate agencies to eliminate EMSEC deficiencies.

3.3.3.9. Ensure the wing commander and appropriate unit commanders are advised of any EMSEC hazards.

3.3.3.10. Conduct meetings with all unit EMSEC monitors as required.

3.3.4. Unit Commanders (responsible for information systems that process classified information) will:

3.3.4.1. Appoint a unit EMSEC monitor. The appointment letter will include the name, rank, office symbol, security clearance and duty phone number of the appointed individual. To fill the position of unit EMSEC monitor, appointees must:

3.3.4.1.1. Maintain a mandatory SECRET security clearance.

3.3.4.1.2. Hold, at a minimum, the grade of E-4 (military) or GS-4 (civilian).

3.3.4.1.3. Have access to a safe or container suitable for storing SECRET materials.

3.3.4.1.4. Know which offices in the unit are required to work with classified national security information. NOTE: Technical expertise in EMSEC is not necessary, but familiarity with classified equipment within the unit is desirable.

3.3.5. Unit EMSEC Monitors will:

3.3.5.1. Identify to the WEM all equipment and facilities used to process classified national security information.

3.3.5.2. Assist the WEM in performing EMSEC inspections.

3.3.5.3. Conduct required EMSEC training within their unit.

3.3.5.4. Coordinate procurements of equipment that will be used to process classified national security information with the WEM.

3.3.5.5. Ensure that the unit commander is briefed on any EMSEC hazards or deficiencies on classified or unclassified systems in the unit.

3.3.5.6. Be the focal point for all EMSEC matters between the WEM and the unit.

3.3.5.7. Ensure all offices in the unit which use classified equipment have this instruction on file.

3.3.5.8. Keep an EMSEC file for each facility processing national security information which will include the following documentation:

3.3.5.8.1. A copy of the unit EMSEC monitor appointment letter.

3.3.5.8.2. A list of classified equipment processors.

3.3.5.8.3. A copy of latest EMSEC assessment.

3.3.5.8.4. A copy of latest EMSEC countermeasures review.

3.3.5.8.5. A copy of any waivers.

3.3.5.8.6. Any related correspondence.

3.3.5.9. Review all AF Forms 3215 that are submitted by the unit. Coordinate each request that relates to a classified information processing system with the WEM and ensure EMSEC considerations have been taken into account prior to forwarding the request.

3.3.5.10. Initiate the completion of, at the request of the WEM, an AF Form 332, **Base Civil Engineer (BCE) Work Request**, and forward it to 45 CES to correct discrepancies.

3.3.6. Base Civil Engineers will:

3.3.6.1. Respond to work requests identified to correct EMSEC deficiencies and will ensure corrective actions are both timely and permanent. For problems beyond local technical expertise, the BCE and the WEM will seek assistance from the HQ AFSPC EMSEC Manager.

3.3.7. All personnel who process classified information electronically will:

3.3.7.1. Keep their unit EMSEC monitors informed of changes to their facility which may affect the EMSEC profile. Some examples of such changes include:

3.3.7.1.1. Removing or installing telephone service.

3.3.7.1.2. Moving equipment to a new location.

3.3.7.1.3. Proposing to or purchasing new equipment.

3.3.7.1.4. Introducing any electronic device into the classified processing area (whether or not it is used to process classified information).

3.3.7.1.5. Construction in adjacent areas that could decrease the controlled space (CS) or the equipment radiation TEMPEST zone (ERTZ).

3.3.7.1.6. Initiate the completion of, at the request of the WEM, an AF Form 332, **Base Civil Engineer Work Request**, and forward it to 45 CES to correct discrepancies.

3.3.8. All personnel will:

3.3.8.1. Refrain from discussing EMSEC vulnerabilities and assessment write-ups (also called discrepancies) over unsecured telephone lines when responding to EMSEC assessments. Some EMSEC discrepancies are considered classified until resolved. STU-III devices are available for classified discussions if necessary.

3.4. **Training.** EMSEC training is available upon request for newly appointed unit EMSEC monitors. Call the EMSEC office for additional information.

3.5. **Contact and Additional Information.** The wing EMSEC manager, 45 SCS/SCBIJ, can be reached at 494-5476 (DSN 854-5476). Information pertaining to wing EMSEC is located on the wing Intranet (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/Emsec/Emsec.htm>).

4. COMPUSEC Program.

4.1. **Overview.** The objective of the COMPUSEC program is to protect and maintain information system resources and information processed throughout the system's life cycle by the use of security measures. Users should reference AFI 33-202 for more detailed information and may obtain assistance and guidance from the WIAO for IA requirements.

4.2. Base Information System Network Accreditation Verification Process.

4.2.1. Systems connecting to either classified or unclassified base network backbones must have a DAA approval and service level agreement (SLA) through the NCC, 45 SCS/SCAB. (The term base network backbone refers to the infrastructure that connects all autonomous networks on the installation or the communications transport that allows connectivity to the Internet.)

4.2.2. The NCC will verify accreditation status of all autonomous systems and networks via the CATS) prior to connection to the base network backbone in accordance with the wing DAA Pro-

cess. (The DAA accreditation approval process flowchart is located on the wing IA Intranet website, https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Accreditation_Info/C&A%20Process%20Jan%2002.jpg.) The NCC will verify accreditation status (i.e., via the CATS) before connection to the either of the base networks.

4.3. Certification and Accreditation.

4.3.1. Department of Defense Information Technology Security C&A Process. The wing has transitioned to the DITSCAP. AFSPC has decreed that extensions to expiring accreditations (in other formats such as AFSSI 5024) will no longer be accepted. All system accreditations or re-accreditations submitted after 1 September 2001 will be submitted in the DITSCAP format unless otherwise authorized by the DAA. The wing will not revoke the accreditation of systems currently accredited under AFSSI 5024.

4.3.2. Information System Accreditation. All Air Force information systems are to be accredited before their operational use. Systems unable to meet Air Force C&A requirements due to the uniqueness of their configuration or mission are not exempt from the accreditation requirement. However, the System Security Authorization Agreement (SSAA) can be tailored to identify the special circumstances; and the DAA can make a decision to accept the risk or deny operability. For example, systems that use a commercial Internet service provider to access the Internet inherit all the vulnerabilities associated with that method of access. Since they have no connectivity to other Air Force systems or networks, the operational risk is acceptable.

4.3.2.1. Personal Digital Assistant Accreditation. PDAs must be accredited before operational use. The WIAO has developed a wing level type accreditation package for all PDAs that meet the applicable requirements. Check the COMPUSEC area of the WIAO Intranet website (https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Accreditation_Info/Accreditation.htm) to see if your PDA is covered by one of these accreditations. PDAs not covered by the wing level package must be accredited separately.

4.3.2.2. Laptop Accreditation. The WIAO has developed a wing level type accreditation package for all laptops that meet the applicable requirements. Laptops not covered by the wing level package must be accredited separately. ISSOs responsible for government laptops will

4.3.2.2.1. Accredite all unit laptops before operational use.

4.3.2.2.2. Complete user acceptance forms for all laptops accredited under the wing type accreditation. Refer to the COMPUSEC section of the WIAO Intranet website (https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Accreditation_Info/Accreditation.htm) to see if your laptop is covered by one of these accreditations.

4.3.2.2.3. Ensure a copy of the signed accreditation letter and user acceptance form is always with each laptop.

4.3.3. Roles and Responsibilities.

4.3.3.1. Designated Approving Authority.

4.3.3.1.1. The 45 SW/CC is the DAA for wing systems. Tenant unit commanders or appointees at higher tenant headquarters are the DAAs for their respective systems. A diagram of the entire DAA process is located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/CompuSec.htm>)

4.3.3.1.2.).

4.3.3.1.3. The DAA will appoint group commanders as DAA representatives.

4.3.3.1.4. When there is a change in the wing commander position, the incoming commander acting as Designated Approving Authority (DAA) will sign an affirmation to continue operations of currently accredited systems.

4.3.3.2. Designated Approving Authority Representative.

4.3.3.2.1. Delegated DAA representatives will assist in the C&A of wing systems. They identify, address and coordinate security accreditation issues with the DAA. A direct link must exist between the DAA representative and the DAA; however, the DAA, not the DAA representative, makes the accreditation decision.

4.3.3.2.2. DAA representatives are authorized to appoint Certifiers for their respective information systems.

4.3.3.3. Certifier (formerly Certifying Official).

4.3.3.3.1. Based on system certification, the certifier (formerly certifying official) makes technical judgments of information system compliance with the systems security policy, and develops an accreditation recommendation for submission to the DAA.

4.3.3.3.2. The Executive Director, Eastern Launch and Test Range (45 SW/TD) is the certifier for information systems and networks supporting launch and range operations.

4.3.3.4. Information System Security Officer. To ensure CATS information is accurate, the ISSO of each system must forward a copy of the signed DAA accreditation letter to the WIAO.

4.4. Information System Use Policy.

4.4.1. Roles and Responsibilities.

4.4.1.1. The WIAO will:

4.4.1.1.1. Be the installation focal point for the monitoring of unauthorized network activity, specifically for evidence of fraud, waste and abuse. If formal investigation is needed, WIAO will contact the IG, Office of Special Investigation or Security Forces. To prevent unauthorized Internet use, the WIAO will periodically review the proxy reports for overall organizational activity trends such as misuse of bandwidth and inappropriate worldwide web surfing.

4.4.1.1.2. Upon finding trends of unauthorized Internet use, issue "Policy Abuse Memos" containing their findings to applicable commanders. Additionally, the WIAO may forward a report of the unit findings to NCC.

4.4.1.1.3. Upon formal request, assist commanders in official investigations involving information systems that store or process government data. The WIAO will be the focal point for requests to use 45 SCS resources such as manpower, time, etc. to retrieve data relative to the investigation from government-owned information systems. Incorporate investigation results into Information Protection Reports and sends them to the requesting units.

4.4.1.1.4. Will request any assistance from the EAOS system administrators by opening

trouble tickets with the Base C4 Help Desk.

4.4.1.1.5. Maintain historical files of incidents for up to two years.

4.4.1.1.6. Direct and coordinate the collection of data for investigations.

4.4.1.2. The Installation Commander may:

4.4.1.2.1. Authorize personnel to look specifically for evidence of fraud, waste, and abuse.

4.4.1.2.2. Authorize real-time monitoring of user account activity. Designees of the installation commander may also authorize account monitoring. NOTE: This authorization does not include unopened E-mail traffic. Only the Secretary of the Air Force/General Counsel (SAF/GC) may authorize real-time monitoring of E-mail traffic.

4.4.1.3. The Designated Approving Authority may:

4.4.1.3.1. Authorize search of information systems in his purview.

4.4.1.3.2. Authorize access to previously read E-mail traffic.

4.4.1.4. Commanders (unit level and above).

4.4.1.4.1. May request proxy reports from the WIAO for systems and users under their purview.

4.4.1.4.2. Will request assistance from the information system network administrator through the WIAO during investigations. To ensure the legality of the request and compliance with AFCA Rules of Engagement (ROE) for System Administrators, commanders will have the applicable legal authority (i.e., 45 SW/JA) review requests.

4.4.1.4.3. Will provide a job order number (JON) in case any additional expense is incurred due to contractor involvement.

4.4.1.4.4. For investigative assistance that involves access to network security/audit records, E-mail, and personal information stored on a government information system, will seek guidance from the local legal authority (e.g., judge advocate).

4.4.1.4.5. May authorize personal use of government resources as allowed by the Uniform Code of Military Justice, Department of Defense 5500.7-R Joint Ethics Regulation. For a listing of unauthorized E-mail and Internet use, visit the WIAO Intranet website, https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/System_Use/System_Use.htm. "Personal" use.

4.4.1.4.5.1. Must not interfere with mission performance.

4.4.1.4.5.2. Must be of a reasonable duration and frequency (e.g., restricted to after-duty hours or personal time).

4.4.1.4.5.3. Must be in the best interest of the Air Force.

4.4.1.4.6. Will appoint ISSOs for each system or flight.

4.4.1.5. Electronic Office Automation System (EOAS) Administrators will:

4.4.1.5.1. Adhere to the Rules of Engagement for System Administrators found on the Air Force Communications Agency website

(https://www.afca.scott.af.mil/ip/info_services/compusec_sec.cfm?COMPID=2).

4.4.1.6. EOAS users are encouraged to visit the WIAO Intranet website, https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/System_Use/System_Use.htm for guidelines on authorized Internet use.

4.5. **Appointment Letters.** Appointments to unit COMPUSEC manager (UCM) (if applicable) and unit ISSO will be made in writing and will be signed by the unit commander. The UCM may appoint an ISSO responsible for individual systems instead of all the systems in a unit. The UCM signature on these appointment letters is sufficient. Forward UCM, ISSO, and other COMPUSEC-related appointment letters to 45 SCS/SCBIN. Recommended format for all appointment letters is located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Appointments/Appointments.htm>).

4.6. **Training.** Once the WIAO receives a copy of the COMPUSEC manager or ISSO appointment letter, the appointee will be added to the WIAO training distribution list. Training for COMPUSEC positions is available on the WIAO Intranet website (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI>) or by contacting the COMPUSEC office, 45 SCS/SCBIN, 494-9412/1571/1430/5365.

4.7. **Contact and Additional Information.** The wing COMPUSEC manager, 45 SCS/SCBIN, may be reached at 494-9412 (DSN 854-9412). COMPUSEC information, publications, templates, examples and answers to frequently asked questions are located on the wing Intranet (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI>).

5. IA Awareness Program.

5.1. **Overview.** The IA awareness program emphasizes IA principles and promotes consistent application of security principles during the use of Air Force information systems. Users should reference AFI 33-204 and may obtain assistance and guidance from the WIAO.

5.2. Roles and Responsibilities.

5.2.1. **Commander.** Unit commanders are encouraged to indorse the IA awareness unit review checklist to substantiate compliance with AFI 33-204. The unit review checklist is not mandatory; commanders may chose to document the review of their programs in whatever manner they choose.

5.3. **IA Awareness Month.** The Air Force will no longer continue the IA Awareness Campaign. Instead, in September 2003 there will be one dedicated IA month with activities covering current various aspects of IA.

5.3.1. To promote IA awareness, wing users are encouraged to submit articles that reflect the IA theme for publication in IA Connection magazine. The WIAO may also publish articles in the monthly IA Awareness newsletter or submit them to AFCA for publication in intercom magazine.

5.3.2. The WIAO will recognize three individuals as IA Professionals of the Year based on the individuals' efforts to promote IA awareness. These individuals will be awarded IA medallions and have their names published in the the WIAO newsletter.

5.4. **Appointment Letters.** Appointments to IA awareness manager will be made in writing and will be signed by the applicable unit commander. Forward IA awareness manager and other related

appointment letters to 45 SCS/SCBIM. Recommended format for all appointment letters is located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Appointments/Appointments.htm>).

5.5. Contact and Additional Information. The wing IA awareness program manager, 45 SCS/SCBIM, can be reached at 494-5365 (DSN 854-5365). IA awareness information, including unit manager training and guidance, IA posters, pamphlets, educational videotapes, and briefings are located on the wing Intranet (https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/IA_Awareness/IA_Awareness.htm).

6. TMAP.

6.1. Overview. Telecommunications monitoring and assessment services are used to determine if any sensitive or classified information transmitted on unsecured and unprotected systems could adversely affect United States operations. TMAP teams document the threat, isolate existing or potential operational security (OPSEC) vulnerabilities and identify procedures to minimize or eliminate those vulnerabilities. All Air Force installations are required to provide legally adequate notice to users of Department of Defense (DoD) telecommunications systems, equipment and devices that use of the aforementioned equipment constitutes consent to TMAP monitoring. The Secretary of the Air Force/General Counsel (SAF/GC) reviews the reports provided by each installation for 100% compliance. Users should reference AFI 33-219 for more detailed information on TMAP services available for their organization, and users may obtain assistance and guidance from the WIAO for IA requirements.

6.2. Roles and Responsibilities.

6.2.1. TMAP Manager.

6.2.1.1. TMAP managers must, on a quarterly basis, comply with the following requirements:

6.2.1.2. Spot-check all telecommunications systems to ensure compliance with AFI 33-219, **Attachment 2**.

6.2.1.3. Upon request, submit a biennial report to 45 SCS/SCBI in accordance with AFI 33-219, attachment 2.

6.2.1.4. Ensure compliance with requirements by checking unit communications resources according to AFI 33-230, *Information Protection Assessment and Assistance Program*, (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/TMAP/TMAP.htm>).

6.2.1.5. TMAP Managers will identify the need for TMAP services for their organizations and make a formal request for them through the WIAO. Managers are also responsible for determining whether TMAP services will be needed on a recurring basis and whether they should be included in base operational plans.

6.2.2. Wing Operations Security Manager. The wing OPSEC manager will work closely with organizational OPSEC and TMAP managers to continuously evaluate the state of wing operations security, determine specific OPSEC weaknesses, and implement and evaluate improvement actions.

6.2.3. Commander. Wing command section and staff offices, each group, and every tenant organization must appoint a single TMAP manager to ensure compliance with the applicable requirements of this instruction. Recommend appointments of unit, flight or section TMAP monitors to

assist the TMAP manager. A template for the letter can be found on the wing Intranet (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/TMAP/TMAP.htm>).

6.2.4. **Contractor.** Contractors must comply with TMAP requirements unless they meet the following criteria: 1) the contractors are not using government furnished equipment; 2) they are not connected to any government telecommunications systems; 3) their contract states that the contractor consents to monitoring but does not have to comply with TMAP requirements (i.e., consent notification method is at the discretion of the contractor). Organizational commanders will review their contracts and task organizational functional area managers to work with their TMAP manager/monitors to report contractor compliance. (The aforementioned criteria do not exempt contractors from compliance with other security disciplines such as COMPUSEC, COMSEC, and EMSEC. Contractors processing government information will adhere to the security guidelines stated in their contracts.)

6.3. **Training.** The WIAO is the office of primary responsibility for TMAP. The wing TMAP manager provides users instructions for TMAP reporting procedures, directed and non-directed computer-based training (CBT), training reporting procedures, and metrics.

6.4. **Appointment Letters.** Appointments to TMAP manager/monitor will be made in writing and will be signed by the applicable unit commander. Forward TMAP manager/monitor appointment letters to 45 SCS/SCBIM. Recommended format for all appointment letters is located on the WIAO Intranet site (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/CompuSec/Appointments/Appointments.htm>).

6.5. **Contact and Additional Information.** For additional information, contact the wing TMAP manager, 45 SCS/SCBIM, at 494-5365 (DSN 854-5365). TMAP information is located on the 45 SW Intranet (<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/TMAP/TMAP.htm>).

EVERETT H. THOMAS, Colonel, USAF
Vice Commander

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

AFPD 33-2, *Information Protection*

AFI 33-202, *Computer Security*

AFI 33-203, *Emissions Security*

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-211, *Communications Security (COMSEC)*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 33-230, *Information Protection Assessment and Assistance Program*

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

AF Form 4160, **Information Assurance Assessment and Assistance Program Criteria**

ASD(C3I) Memorandum, 20 March 1997

Office of the ASD(C3I) Memorandum, 11 May 1998

Abbreviations and Acronyms

45 SCS—45th Space Communications Squadron

45 SW—45th Space Wing

45 SWI—45th Space Wing Instruction

ADPE—Automated Data Processing Equipment

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFSSI—Air Force System Security Instruction

AFSSM—Air Force Systems Security Memorandum

ASD—Assistant Secretary of Defense

ASD(C3I)—Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

C&A—Certification and Accreditation

C3I—Command, Control, Communications, and Intelligence

CATS—Certification and Accreditation Tracking System

CBT—Computer Based Training

CCAFS—Cape Canaveral Air Force Station

CO—Certifying Official
COMPUSEC—Computer Security
COMSEC—Communications Security
CRO—COMSEC Responsible Officer
CSSO—Computer System Security Officer
DAA—Designated Approving Authority
DoD—Department of Defense
DSN—Defense Switched Network
EMSEC—Emissions Security
EOAS—Electronic Office Automation System
FOUO—For Official Use Only
FPCON—Force Protection Condition
FRO—Fortezza Responsible Officer
HQ AFCA—Headquarters, Air Force Communications Agency
IA—Information Assurance
IAAP—Information Assurance Assessment Program
INFOCON—Information Operations Condition
ISSO—Information Systems Security Officer
MAJCOM—Major Command
NCC—Network Control Center
NIPRNET—Non-secure Internet Protocol Router Network
OPR—Office of Primary Responsibility
SA—System Administrator
SATE—Security Awareness Training and Education
SIPRNET—Secret Internet Protocol Router Network
SRO—STU/STE Responsible Officer
SSAA—System Security Authorization Agreement
STE—Secure Telephone Equipment
STU—Secure Telephone Unit
TMAP—Telecommunications Monitoring and Assessment Program
UCM—Unit COMPUSEC Manager
WIAO—Wing Information Assurance Office

Attachment 2**INFORMATION ASSURANCE WORLD WIDE WEB RESOURCES**

- A2.1. The 45 SW Information Assurance Office (45 SCS/SCBI)**
–<https://pafbweb.patrick.af.mil/45MXG/45SCS/SCB/SCBI/Default.htm>.
- A2.2. Air Force Communications Agency (AFCA)** –<https://www.afca.scott.af.mil/>.
- A2.3. Air Force Computer Emergency Response Team (AFCERT)** –<http://afcert.kelly.af.mil/>.
- A2.4. Computer Emergency Response Team (CERT)** –<http://www.cert.org/>.
- A2.5. Department of Defense Computer Emergency Response Team (DoD CERT)**
–<http://www.cert.mil/>.
- A2.6. Computer Security Resource Clearinghouse (CSRC)** –<http://csrc.ncsl.nist.gov/>.
- A2.7. DOD Information Assurance Support Environment (IASE)**
–<http://matthe.iiie.disa.mil/index.html>.
- A2.8. HQ Air Force Space Command Information Assurance Office**
–<https://midway.peterson.af.mil/infoprotect/>.
- A2.9. Secret and Below Interoperability (SABI)** –<http://www.sabi.org/>.