BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-219

15 MAY 2000

Communications and Information

TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM (TMAP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AIA/DO (Andra Calder)
Supersedes AFI 33-219, 18 June 1998.

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 22
Distribution: F

This instruction prescribes responsibilities, procedures, and guidance concerning the United States Air Force (USAF) telecommunications monitoring and assessment program (TMAP). It implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and national and Department of Defense (DoD) directives pertaining to the monitoring of unsecured telecommunications and establishes a requirement for feedback in the operational security (OPSEC) process AFPD 10-11, *Operations Security*). Guidance in Air Force Instruction (AFI) 71-101, Volume 2, *Protective Service Matters,* concerning telephone interception and eavesdropping do not apply to telecommunications monitoring conducted according to this instruction. The term major command (MAJCOM) includes field operating agencies, and direct reporting units. This instruction applies to personnel, including civilians under contract by the DoD, who use DoD telecommunications. It only applies to official activities of United States government organizations. Refer questions on the content of this instruction to Headquarters Air Intelligence Agency (HQ AIA)/DO, 102 Hall Blvd., Suite 229, Kelly AFB TX 78243-7029. **Failure to observe the prohibitions and mandatory requirements of this instruction, as set forth in paragraphs 21.6 and 21.7, by military personnel is a violation of Article 92, Uniformed Code of Military Justice. Violations by civilian employees may result in administrative or disciplinary action without regard to other applicable criminal or civil sanctions for violations of related laws.** Refer suggested changes or conflicts between this and other instructions on AF Form 847, **Recommendation for Change of Publication,** to Headquarters Air Force Communications Agency (HQ AFCA)/ITPP, 203 West Losey Street, Room 1065, Scott AFB IL 62225-5233. **Attachment 1** contains a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2000-1, which replaces **Attachment 1** and paragraph A2.3.5. in **Attachment 2**. The change in **Attachment 2** provides the updated notice and consent log-on banner notification statement.

Section A— Telecommunications Monitoring and Assessment Program (TMAP)

1. Telecommunications. The Air Force uses unsecured telecommunications systems such as telephones, cellular phones, radios, facsimile, and computer networks to conduct day-to-day official business. Adversaries can easily monitor these unsecured systems that could provide information on military capabilities, limitations, intentions, and activities.

2. Telecommunications Monitoring And Assessment Program Services. The Air Force monitors unsecured telecommunications systems to determine if these unsecured systems were used to transmit sensitive or classified information. Information collected is analyzed to determine if any sensitive or classified information transmitted on unsecured systems could adversely affect United States (and allied/coalition) operations. Information can be provided near-real-time as a force protection tool or systematically collected, analyzed, databased, and reported to MAJCOMs as long-term information liabilities. The TMAP services, consisting of monitoring telecommunications and assessing monitored data, are available on a routine basis, and during exercises, crises, contingencies, and conflicts. The monitoring and subsequent assessing of data are designed to thoroughly examine communications systems procedures associated with a specific weapon system, operation or activity, and document their vulnerability to hostile signal intelligence exploitation. Through systematic data assessment and analytical procedures, TMAP teams document the foreign hostile threat; isolate existing or potential OPSEC vulnerabilities; and identify procedures to minimize or eliminate OPSEC vulnerabilities. TMAP services are not inspections. The TMAP is an integral part of the USAF OPSEC program. Although the TMAP is considered a wartime mission, it is a very effective tool for a Commander's use during day-to-day operations and exercises to identify real world problems that can adversely affect OPSEC and the warfighter's effectiveness. During the assessments, items such as stereotyped patterns or administrative and physical security procedures routinely surface as possible sources of intelligence losses. The Commander's OPSEC office receives these items as a professional courtesy. The assessment provides the consumer with a product that defines, investigates, and offers specific procedures for correction of problem areas.

3. Telecommunications Monitoring And Assessment Program Reports. TMAP reports provide operational commanders and planners with near-real-time reports of classified or sensitive information disclosures that may adversely affect United States (and allied/coalition) operations. Operational commanders and planners should use these reports for evaluating the effectiveness of OPSEC measures, and developing measures to diminish the value of disclosed information. They may also use these reports to identify and focus training requirements and to justify developing and funding corrective actions.

4. Telecommunications Monitoring And Assessment Program Authority. HQ AIA TMAP elements (including its gained reserve units), are the only USAF organizations authorized to conduct TMAP activities. They perform TMAP activities in a manner that satisfies the legitimate needs of the Air Force to provide OPSEC while protecting the privacy, legal rights, and civil liberties of those persons whose communications are subject to TMAP monitoring.

Section B— Responsibilities

5. The Assistant Secretary of Defense, Command, Control, Communications and Intelligence (ASD/C3I). This individual has sole approval authority for TMAP operations within the Office of the Secretary of Defense and the Defense Telecommunications Service-Washington (DTS-W). DTS-W pro-

vides telecommunications services to DoD elements located in the National Capital Region (NCR). The NCR includes the District of Columbia, Montgomery, and Prince George's counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William counties in Virginia; and the cities of Alexandria, Fairfax, and Falls Church in Virginia. An organization requiring monitoring in the DTS-W area sends its request to HQ AIA/DO at least 90 days prior to the requested monitoring dates, and provides information copies of the request to HQ USAF/XOO, 1630 Air Force Pentagon, Room 4E1046, Washington DC 20330-1630 and Headquarters Air Force Communications and Information Center (AFCIC)/SYN, 1250 Air Force Pentagon, Room 4A1088E, Washington DC 20330-1250. HQ AIA/DO reviews the request as soon as possible, and if capable of supporting the request, pursues the ASD/C3I approval.

6. The Secretary of the Air Force General Counsel (SAF/GC). Biennially, during even-numbered fiscal years, SAF/GC reviews information provided pursuant to the procedures outlined in **Attachment 2**. They authorize TMAP monitoring at those installations that provided adequate notice that using official telecommunications devices constitutes consent to TMAP monitoring.

7. HQ USAF/XOO. This office is the lead office within the Air Force for OPSEC and TMAP operations, and has designated HQ AIA to conduct TMAP services.

8. HQ AFCIC/SYN. This office is the lead office within the USAF for policy matters affecting TMAP and related issues. They coordinate with Joint Staff, National Security Agency, or other DoD components for monitoring telecommunications systems that carry both USAF and other government agency information.

9. Major Commands:

9.1. Continuously evaluate OPSEC measures to determine specific OPSEC weaknesses, and implement and evaluate improvement actions. OPSEC is a special interest item for all MAJCOM Inspector General and Quality Assessment Teams under their "common core criteria."

9.2. Make sure base/facility notification and consent actions are in compliance with Section C and **Attachment 2**.

9.3. Include TMAP services in appropriate operations and exercise plans.

9.4. Request TMAP services from HQ AIA according to Section D.

10. Base/Facilities/Organizations:

10.1. Continuously evaluate the state of security of their operations, determine specific OPSEC weaknesses, and implement and evaluate improvement actions.

10.2. Establish and accomplish notice and consent procedures according to Section C and **Attachment 2**.

10.3. Send annual requests for TMAP services to their respective MAJCOMs.

10.4. Include TMAP services in appropriate operations and exercise plans.

10.5. Appoint an office of primary responsibility (OPR) to coordinate the activities of the TMAP team when scheduled to receive TMAP services. The OPR will:

10.5.1. Stay familiar with the operation under study.

10.5.2. Possess security clearances equal to the classification of the operation studied.

10.5.3. Keep familiar with TMAP objectives and methods.

10.5.4. Help with the arrangements for billeting, transportation, messing, and provide a work area and secure storage facility for the TMAP team.

10.5.5. Help the TMAP team in determining proper classification of report content and report classification authority when required.

10.5.6. Provide necessary technical information when requested, such as frequencies, system specifications, circuit listings, and critical nodes.

10.5.7. Coordinate with appropriate personnel to obtain access to their facilities and their support in all aspects of a TMAP mission. If necessary, arrange funding for local telephone exchange connection fees.

10.5.8. Make sure administrative communications capabilities are available to TMAP teams for operations and administrative support.

10.5.9. Help arrange specialized communications support as needed to meet mission requirements.

10.5.10. Restrict knowledge of the TMAP scheduled activities to those with a need-to-know.

10.5.11. Make sure the appropriate commanders are advised of impending TMAP activities.

10.5.12. Give TMAP personnel access to operational orders and plans, operating instructions, and other mission related documents. Also, make sure the team has access to OPSEC training documents, programs, circuit diagrams, radio logs, traffic records, and other needed documents.

11. HQ AFCA/GCI:

11.1. Notifies MAJCOM Information Protection (IP) offices in early February during even-numbered fiscal years to initiate biennial notification procedures.

11.2. Acts as the focal point for the notice and consent certification process.

12. HQ AIA:

12.1. Develops, funds, procures, and maintains modern TMAP capabilities to support current and future USAF operations.

12.2. Promotes TMAP awareness to MAJCOMs and subordinate organizations, as requested.

12.3. Selects specific HQ AIA units or specific elements within HQ AIA to conduct TMAP activities. Only specifically selected HQ AIA units or elements may engage in TMAP activities.

12.4. Coordinates with HQ AFCA to obtain biennial notice and consent determinations.

12.5. Interacts with Tactical Deception activities to consider ways to turn OPSEC weaknesses to friendly advantage through deception.

12.6. Integrates TMAP services into Air Force-wide OPSEC programs.

12.7. Maintains awareness of changing threats to friendly telecommunications and informs supported Air Force activities of trends and potentially dangerous situations.

12.8. Performs TMAP activities only at installations that SAF/GC has certified notice and consent procedures.

Section C— Notice and Consent Procedures

13. General Notification. General notification is hereby given to Air Force users of DoD telecommunications systems or devices. DoD provides such systems and devices for conducting official government business. They are subject to telecommunications monitoring. Using government telecommunications systems and devices constitutes the users consent to telecommunications monitoring.

14. Performing Telecommunications Monitoring And Assessment Program Functions. HQ AIA only performs TMAP functions at locations in compliance with notice and consent procedures prescribed in this instruction and certified by the SAF/GC.

15. Notice and Consent Certification Process.

15.1. Host Communications Units. The communications unit at each Air Force installation prepares a detailed summary (Reports Control Symbol (RCS): HAF SC(BE)9497, Summary of Consent Notification Actions) of the previous 24-month actions to follow notice and consent procedures described in **Attachment 2**. It sends the summary to the installation Staff Judge Advocate (SJA) by 15 April each even-numbered fiscal year. This report is designated emergency status code C-3. Continue reporting during emergency conditions, delayed precedence. Submit data requirements as prescribed, but higher precedence report submissions may cause delays. Send by non-electronic means, if possible. Summaries covering more than one installation must clearly identify each installation, and the description of each notification action must indicate how the action applies to each installation. Installation officials and their action officers should make their personnel aware that the United States Government frequently transmits information via radio, which makes the information readily susceptible to interception and analysis by our adversaries. As a minimum, complete and document the actions outlined in **Attachment 2** in order to further SAF/GC certification of the installation's notice and consent procedures. An example of a summary letter is in **Attachment 3**. Upon receipt of SJA indorsement, the host communications unit sends it, along with the base summary, to their MAJCOM IP office.

15.2. Installation Staff Judge Advocates. The installation SJA reviews the summary and determines, in writing (see SJA 1st Ind, **Attachment 3**), that the actions described are legally sufficient to provide notice that using DoD telecommunications constitutes consent to telecommunications monitoring. The SJA then sends a written determination to the host communications unit.

15.3. MAJCOM Information Protection Offices. These offices make sure all bases and installations under their control have responded, and send all base summaries and SJA determinations to MAJCOM/SJA for their notice and consent determinations. IP offices then forward all summary letters (without attachments) and SJA 1st indorsements to HQ AFCA by 1 May of each even-numbered fiscal year.

15.4. HQ AFCA Information Protection Office. Makes sure all USAF facilities submit inputs in order to receive the biennial SAF/GC certification. They send all summaries and SJA determinations to the HQ AFCA/SJA for their review. The IP office then sends all such summaries of actions to SAF/GC by 15 July each even-numbered fiscal year.

15.5. SAF/GC. Certifies that legally sufficient prior notice was given to users of USAF telecommunications systems of specific installations and that TMAP activities are authorized at those installations. They provide a certification listing to HQ AFCA by 1 September of each even-numbered fiscal year, of the installations approved to receive TMAP services. This certification listing is valid beginning 1 October, for two fiscal years. They provide reasons why other installations were disapproved TMAP certification.

15.6. HQ AFCA sends the SAF/GC information to HQ AIA/DO and MAJCOM IP offices. HQ AFCA works with MAJCOM IP offices to ensure that installations not certified by SAF/GC as meeting the notice and consent requirements, accomplish whatever actions were determined incomplete or deficient, and resubmit for SAF/GC reevaluation and determination.

15.7. HQ AIA/DO sends the SAF/GC certification listing of installations to affected HQ AIA units by 15 September of each even-numbered fiscal year.

Section D— Requesting Telecommunications Monitoring And Assessment Program Services

16. Soliciting. HQ AIA solicits requests for TMAP services each January.

17. Tasking Priority. HQ AIA and designated subordinate organizations use the following order of mission priorities to best use limited TMAP resources:

17.1. Real world contingency operations.

17.2. Real world non-contingency operations.

17.3. Joint Chiefs of Staff (JCS) exercises.

17.4. Exercises in support of Operations Plans/Contingency Plans under which a HQ AIA TMAP element is tasked.

17.5. Operational test and evaluation activities.

17.6. Tactical Evaluation/MAJCOM exercises, etc.

17.7. Numbered Air Force exercises.

17.8. All other requests.

18. Joint Chiefs of Staff Support. JCS policy tasks the military services to furnish telecommunications monitoring support for JCS exercises or operations. HQ AIA gives support to unified and specified commands in joint and allied combat situations and exercises, as requested in the Air Force component command's operations plans or directives. Unified or specified commands send requests for telecommunications monitoring to the theater Intelligence Group, through the Air Force component commander, if appropriate, with information copies to HQ USAF/XOO, and HQ AIA/DO.

19. Out-Of-Cycle Requests. Occasionally, unscheduled MAJCOM TMAP requests arise. Examples are real-world contingencies or short-notice exercises. Send all requests for TMAP support during contingencies by message to HQ AIA/DO. Submit other requests by message to the 67th Intelligence Wing (67 IW KELLY AFB TX//CC//) and the appropriate theater Intelligence Group which will make every effort to support out-of-cycle requests. Organizations collocated with HQ AIA TMAP elements may submit unscheduled short-notice requests directly to the HQ AIA unit within its area of responsibility, when time

does not permit submission to the 67 IW first. These organizations should make sure their parent organization is cognizant of their request and coordinate any needed report distribution arrangements.

20. Threat Consideration. By 1 September of each year, the Air Force Information Warfare Center (AFIWC) evaluates the threat to requesting units' communications and furnishes that data to the appropriate theater Intelligence Group. The AIA TMAP element considers the threat data when prioritizing MAJCOM requests. Address threat assessments in all TMAP reports. The reporting requirement in this paragraph is exempt from licensing according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections.*

Section E— Telecommunications Monitoring And Assessment Program Procedures

21. HQ AIA Telecommunications Monitoring And Assessment Program Per sonnel Will:

21.1. Comply with applicable Federal laws, National, DoD, and JCS policy, and this instruction. **Failure to observe the prohibitions and mandatory requirements set out in paragraph 21.6. and 21.7., by military personnel is a violation of Article 92, Uniformed Code of Military Justice. Violations by civilian employees may result in administrative or disciplinary action without regard to other applicable criminal or civil sanctions for violations of related laws.**

21.2. Monitor and assess DoD/USAF telecommunications to satisfy legitimate Air Force operational requirements.

21.3. Conduct TMAP activities only on DoD-owned or leased telecommunications systems/devices.

21.4. Only target official telephone lines. For example, do not monitor class B (on-base quarters) telephones.

21.5. Not use tone-warning devices when using recording equipment for TMAP activities.

21.6. Not intentionally report, or file any acquisition or proprietary information, or personal privacy information (PPI) extraneous to the TMAP activity, or any privileged information such as confidential communications between attorney and client, husband and wife, or clergy and penitent.

21.7. Promptly destroy any information inadvertently collected except if it: 1) relates to an intrusion, or to activities that are likely to impair the efficiency of the system or are likely to enhance system exposure to intrusions; or 2) reveals an emergency situation or situation threatening grievous bodily harm; or significant loss of property. Inadvertently collected information that is not destroyed shall be reported according with the provisions of paragraph 24.5.

21.8. Comply with reporting and handling procedures outlined in this instruction to advise supported commanders of problems identified through TMAP activities.

Section F— Telecommunications Monitoring And Assessment Program Reports

22. AIA Telecommunications Monitoring And Assessment Program units send reports as specified by the requester. When TMAP activities are accomplished in conjunction with OPSEC surveys, include TMAP reports as part of the OPSEC survey report. There are two basic types of reports:

22.1. Telecommunications Monitoring Report (TMR). A timely, usually brief report, used to notify the consumer of suspected intelligence disclosures. These reports may contain intentional or uninten-

tional compromises of classified information, classified or unclassified information of possible immediate or short term intelligence value to Hostile Intelligence Service, CI, and information pertaining to very important persons' movements. The reporting requirement in this paragraph is exempt from licensing according to AFI 33-324.

22.2. Telecommunications Assessment Report (TAR). Provides the consumer with a summary of problem areas or possible intelligence losses noted during telecommunications assessments and telecommunications monitoring missions. The TAR is issued at varying intervals during the mission to meet consumer needs and at the end of a project. Since telecommunications assessments may take a long time and since assessment reports often require corroboration with the involved organizations, report preparation may take longer than reports for less comprehensive projects. The consumer establishes the distribution requirement of the report. Circulate a copy of the final report within HQ AIA channels for oversight, quality control, and to extract statistics of TMAP activities. The reporting requirement in this paragraph is exempt from licensing according AFI 33-324.

Section G— Using and Controlling Telecommunications Monitoring And Assessment Program Information

23. Uses and Restrictions. Use information in the TMAP reports only for official United States government TMAP purposes, except as noted in this instruction. Using TMAP reports for other than official TMAP purposes may violate public law as well as DoD, JCS, and Air Force directives. Personnel handling TMAP reports must protect the rights of individuals and proprietary information. This principle and restriction on use are equally applicable and binding upon both producers and consumers of TMAP reports, as well as other individuals who may come into contact with information contained in those reports, without regard to rank, status, or position.

23.1. HQ AIA personnel use information developed from monitored telecommunications as the basis for issuing reports to consumers for official TMAP purposes. However, certain restrictions apply to the report content. These reports will not include identifying data such as names of conversants, office symbol, telephone circuits, or any other data that could reasonably identify a conversant. Include the names of personnel who are not conversants when those names are an integral part of reporting the intelligence loss. TMAP reports will not contain transcripts of conversations, reproductions of monitored facsimiles or e-mail transmissions, but may include short extracts or quotes when necessary to clarify the information reported.

23.2. Do not use the results of TMAP services to produce foreign intelligence or counterintelligence information.

23.3. The results of TMAP services are used for intelligence exercise purposes in some instances. During telecommunications monitoring support to exercises, the exercise director may request release of TMAP reports derived from the monitoring of friendly communications to Opposition Forces (OPFOR). Release TMAP reports generated during an exercise to the OPFOR only under the following guidelines:

23.3.1. Reports must retain their identity as TMAP reports.

23.3.2. Do not identify or pass TMAP intelligence information to the OPFOR as signals intelligence.

23.3.3. Do not include information extraneous to TMAP purposes.

23.3.4. Do not identify conversants.

23.3.5. The exercise director determines dissemination. Expressly state dissemination controls on each report.

24. Requesting and Releasing Telecommunications Monitoring And Assess ment Program Information and Transcripts. The reporting requirement in this paragraph is exempt from licensing according to AFI 33-324.

24.1. Air Force consumers may request transcripts of monitored communications from the HQ AIA organization submitting a report if it reveals possible security violations or CI disclosures that may impact on operational capabilities. Upon request, HQ AIA units release sanitized transcripts of monitored communications to the consumer. Sanitized transcripts are true representations of the communication in every respect except they must not contain names or any data that identifies conversants, and must not contain personal privacy or proprietary information. Sanitize electronic mail and facsimile messages and provide in summary format only. After reviewing sanitized transcripts, the consumer may request unsanitized transcripts by certifying, in writing, to HQ AIA/DO, that a security violation has occurred. If HQ AIA/DO's evaluation determines the release of names and identifying data is justified, they direct the TMAP element to send the unsanitized transcripts to the requesting agency. TMAP elements may only provide unsanitized transcripts to requesters authorized to review them by statute, Executive Order, or DoD Policy.

24.2. TMAP elements may release sanitized transcripts to exercise directors and supported commanders during TMAP missions supporting joint service or unified command exercises or operations. TMAP elements may also release unsanitized transcripts to joint or unified command authorities, when reviewed and approved according to the procedures outlined by the governing directives of the service designated as executive agent for the mission. During exercises and peacetime operations, HQ AIA TMAP elements advise HQ AIA/DO of the circumstances when releasing unsanitized transcripts to joint or unified command authorities.

24.3. Occasionally, information involving other DoD components or civil agencies is disclosed while monitoring Air Force activities. When this occurs, provide the transcript to HQ AIA/DO for further processing. DoD components requiring transcripts must send requests to HQ AIA/DO. If approved, HQ AIA/DO provides these transcripts only after removing data that identifies Air Force personnel.

24.4. HQ AIA TMAP resources occasionally participate in exercises and operations conducted with an allied nation or coalition of allied nations, such as the North Atlantic Treaty Organization. HQ AIA TMAP personnel must avoid discussions that reveal specific United States weaknesses and capabilities. When an AIA activity performs a TMAP mission in an allied environment or is tasked to take part in a multinational monitoring mission, controlling recorded media and releasing transcripts must follow procedures set up by the executive agency for the particular exercise or operation. Unsanitized transcripts containing United States persons' conversations are not releasable outside the allied telecommunications monitor cell without HQ AIA/DO approval as outlined above.

24.5. Information acquired inadvertently during the course of an authorized TMAP operation that reveals an emergency situation or situation threatening death or grievous bodily harm must be immediately reported to the military commander, the Air Force Office of Special Investigations (AFOSI), or other law enforcement agency having appropriate jurisdiction. Use the most expeditious means available that provides adequate security. This is not a TMAP report, consequently, do not issue a

TMR or TAR. Do not include information pertaining to these incidents in any of the reports of the TMAP mission. The TMAP element must give complete details, by message, within 24 hours of initial AFOSI notification to HQ AIA/DO/JA with information copies to 67 IW/CC, 248 Kirknewton St, San Antonio TX 78243-7150, and their parent unit. Refer information acquired inadvertently during the course of an authorized TMAP operation that relates directly to a significant crime, or to significant fraud, waste, or abuse, except those communications protected by the attorney-client privilege, to the military commander, AFOSI, or law enforcement agency having appropriate jurisdiction over the unit you are monitoring. Notify SAF/GC promptly of any such referrals.

24.6. HQ AIA TMAP units must report disclosures involving high-level distinguished visitors (DV) movements, DV-3 or higher, to the local AFOSI. DV 1-3 personnel include the President, Vice President, Cabinet members, Senators and Congressmen, foreign heads of state and ambassadors, military grade of General, and Senior Executive Service personnel. Classify reports identifying such movements in accordance with the Foreign Clearance Guide for overseas travel and FOR OFFICIAL USE ONLY within the continental United States. Specific itineraries may carry higher classifications based on trip sensitivity.

24.7. Upon request, HQ AIA TMAP elements may release recorded telecommunications of monitoring missions to the 312th Technical Training Squadron for TMAP training. In this respect, the 312th Technical Training Squadron will:

24.7.1. Control access to the recorded telecommunications.

24.7.2. Label the recorded telecommunications as containing information obtained through telecommunications monitoring.

24.7.3. Inform all students and instructors, in writing, that the recorded telecommunications are only for classroom discussion.

24.8. The reporting requirement in this paragraph is exempt from licensing according to

AFI 33-324.

25. Using Telecommunications Monitoring And Assessment Program Information for Law Enforcement and Punitive Actions. Air Force activities must not use TMAP information for any law enforcement purpose, except as noted in paragraph **24.5.** (inclusive). Receiving units may only use identifying data for preventive actions or for administrative actions taken for unauthorized disclosure of classified national security information. For punitive/legal actions beyond the scope of administrative actions, units must submit the matter through HQ AIA/DO/JA to HQ AFCIC/SYN, and SAF/GC, 1740 Air Force Pentagon, Room 4E856, Washington DC 20330-1740. Do not use TMAP operations results in a criminal prosecution without prior consultation with SAF/GC.

Section H— Releasing Telecommunications Monitoring And Assessment Program Information to Enhance OPSEC Awareness and Education

26. Supporting Operation Security Awareness and Education . Improving operations security within the Air Force depends in large upon maintaining OPSEC awareness and education. HQ AIA TMAP elements may provide extracts of TMAP reports and brief quotes or extracts from monitored telecommunications to support OPSEC awareness and education. Typically, extracts include examples of user's communications practices that endanger or enhance OPSEC. AFIWC/OS develops this informa-

tion for use in the Air Force OPSEC program. AFIWC provides information for educational purposes in response to a specific request, or the AIA unit may provide monitored information that supports OPSEC awareness and education. HQ AIA TMAP elements may also provide such information directly to consumers when requested. All restrictions on releasing identifying data apply to releasing extracts. If extracted communications from outside the requesting organization are required to meet the consumer's need, the extracts will not identify the base or organization involved in the monitored telecommunications.

27. Form Prescribed . This AFI is the prescribing directive for DD Form 2056, **Telephone Monitoring Notification Decal**.

GARY A. AMBROSE, Brig Gen, USAF
Acting Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

DoDD 8000.1, *Defense Information Management (IM) Program*

AFPD 10-11, *Operations Security*

AFPD 33-2, *Information Protection*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

AFI 71-101, Volume 2, *Protective Service Matters*

OASD/C3I, *Memorandum, Communications Security (COMSEC) Monitoring,* 14 April 1999

Abbreviations and Acronyms

67 IW—67th Intelligence Wing

AFCA—Air Force Communications Agency

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AIA—Air Intelligence Agency

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

ASD—Assistant Secretary of Defense

CI—Critical Information

C3I—Command, Control, Communications, and Intelligence

DoD—Department of Defense

DTS—Defense Telecommunications Service

DV—Distinguished Visitor

IP—Information Protection

JCS—Joint Chiefs of Staff

MAJCOM—Major Command

NCR—National Capital Region

OPFOR—Opposition Forces

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PPI—Personal Privacy Information

RCS—Reports Control Symbol

SAF—Secretary of the Air Force

SJA—Staff Judge Advocate

TMR—Telecommunications Monitoring Report

TAR—Telecommunications Assessment Report

TMAP—Telecommunications Monitoring and Assessment Program

USAF—United States Air Force

Terms

Consumer—Normally the Air Force unit identified to receive support, i.e., the requesting MAJCOM, or a subordinate unit at any level of command.

Critical Information (CI)—Information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage. Such information if released prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause loss of lives and/or damage to friendly resources.

Information Systems—a. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual (DoDD 8000.1, *Defense Information Management (IM) Program*). b. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. (AFPD 33-2, *Information Protection*).

Notice and Consent—A notification program that includes all actions taken to make sure users of official DoD telecommunications systems/devices are adequately notified that using official DoD telecommunications systems/devices constitutes consent to telecommunications monitoring.

Open Information Systems—Any information system or activity that is accessed or observed by personnel outside the system and provides information by open sources or OPSEC indicators. Open information systems use open source information to provide OPSEC indicators that may be observed by adversaries. Open information systems may also be influenced, jammed, interrupted, or exploited by adversaries and adversarial weapons systems. Examples are nonsecured telephone systems, computer systems connected to outside lines, and unsecured radio systems.

Personal Privacy Information (PPI)—Any item, collection or grouping of information about an individual's private or personal affairs, including (but not limited to) personal financial matters, social behavior, medical conditions, or any other information, the release of which would be considered an unwarranted invasion of the individual’s privacy.

Requester—Normally a MAJCOM that requests TMAP support. On certain occasions, a requester could be HQ AIA, HQ AIA theater wings, or Air Force operational units down to wing level.

Telecommunications—Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems (JP 1-02).

Telecommunications Assessment—An evaluation of telecommunications to identify, analyze and report inadvertent disclosures of classified/sensitive information.

Transcript—A verbatim typewritten reproduction of a monitored communication including (if contained in the communication) conversants' names, telephone numbers, circuit designators, organizations, call signs, and other identifying data. Any explanatory or other comments included in a transcript are clearly offset and indicated as such so they are not construed as part of the transcribed communication. The following terms also apply to transcripts:

Sanitized Transcript—A transcript that was edited to remove the names of conversants and any other data that could reasonably identify conversants.

Unsanitized Transcript—A term that means the same as transcript. It is used when needed to clearly discriminate between transcript and sanitized transcript.

Unsecured Telecommunications—Telecommunications which do not use authorized cryptographic products or protected distribution systems.

Addresses

67 IW/CC

248 Kirknewton St

San Antonio TX 78243-7150

HQ AFCA/ITPP

203 West Losey Street, Room 1065

Scott AFB IL 62225-5222

HQ AFCIC/SYN

1250 Air Force Pentagon, Room 4A1088E

Washington DC 20330-1250

HQ AIA/DO

102 Hall Blvd, Suite 229

Kelly AFB TX 78243-7029

HQ USAF/XOO

1630 Air Force Pentagon, Room 4E1046

Washington DC 20330-1630

SAF/GC

1740 Air Force Pentagon, Room 4E856

Washington DC 20330-1740

Attachment 2

NOTICE AND CONSENT PROCEDURES

A2.1. Educate personnel about the hostile signals intelligence threat to unsecured telecommunications.

A2.2. Provide guidance to users in the proper use of unsecured telecommunications.

A2.3. Notify users of DoD telecommunications, including contractors and their employees, that using United States government telecommunications systems constitutes consent to telecommunications monitoring. The following notification procedures are ***mandatory*** for official United States government telecommunications systems/devices:

A2.3.1. Installation telephone directories. Prominently display a consent statement on the front cover of telephone directories.

A2.3.2. Telephones: Affix DD Form 2056, **Telephone Monitoring Notification Decal**, on all telephones subject to telecommunications monitoring. This includes telephones with secure voice capability that can be used in the unsecure mode, such as STU-IIIs.

A2.3.3. Facsimile Machines. Either of the two following notification actions is considered sufficient notification to users of facsimile machines:

A2.3.3.1. Apply a sticker, similar to the DD Form 2056, on all facsimile machines stating, "This device is subject to monitoring at all times. Using this device constitutes consent to monitoring."

A2.3.3.2. Require mandatory use of AF Form 3535, **Facsimile Electro Mail Transmittal**, with a notice and consent statement, i.e., "Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using DoD telecommunications systems constitutes consent to monitoring."

A2.3.4. Cellular Telephones and Hand-held Radios. Hand-held radios and cellular phones are extremely susceptible to hostile intercept, and therefore, are valuable indicators to monitor for security assessment purposes. Because of their physical size, excessive handling, and the tactical environment (heat/dirt/humidity) they are subjected to, either of the two following notification actions is considered sufficient notification to cellular phone and hand-held radio users:

A2.3.4.1. Affix DD Form 2056, or a similar form, to the phone/hand-held radio or:

A2.3.4.2. Require personnel to sign a notification and consent form when issued a cellular phone or hand-held radio. The form will state, i.e., "Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using this telecommunications system or device constitutes consent to monitoring. I have read, understand and consent to the aforementioned statements of telecommunications monitoring."

A2.3.5. Put users of Air Force computer systems on notice that system use constitutes consent to monitoring and system testing. Install a notice and consent log-on banner on all computers. At the minimum, proper notification in terms of content is:

"This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for autho-

rized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

A2.4. Optional methods to get this information to Air Force personnel are:

A2.4.1. Correspondence from the base or facility commander, addressing proper use of unsecured telecommunications, to all assigned units for dissemination to unit personnel.

A2.4.2. Addressing telecommunications issues to newcomers during in processing, periodic OPSEC awareness briefings, and commander's calls.

A2.4.3. Using base bulletins and similar publications on a periodic basis.

A2.4.4. Incorporating notice and consent comments in operating procedures, instructions, etc., that are periodically reviewed by users.

A2.4.5. Placing a (red) adhesive label that states, "This telecommunications device is subject to monitoring at all times. Using this device constitutes consent to monitoring."

A2.4.6. Any other actions deemed appropriate by the base or facility commander or the commander's designee to make sure DoD telecommunications systems users are aware that using these systems and devices constitutes consent to telecommunications monitoring.

Attachment 3

EXAMPLE OF NOTICE AND CONSENT MEMORANDUM AND 1ST IND

MEMORANDUM FOR 123 FIGHTER WING/JA

FROM: 123 COMMUNICATIONS SQUADRON

123 S. Galaxy St, Room 1025

HOMESTEAD AFB FL 33548

SUBJECT: Summary of Consent Notification Actions Taken 1 Apr 92 - 31 Mar 94 (RCS: HAF-SC(BE)9497

The following actions were taken during the past two years to notify Air Force users of DoD telecommunications that using the telecommunications constitutes consent to telecommunications monitoring.

a. The current base telephone directory, dated January 1994, includes the consent notice on the front cover. (see Attachment 2)

b. The requirement to have the DD Form 2056 affixed to telephones was periodically briefed. In order to verify that telephones have the DD Form 2056 attached, a random visual survey was conducted in August 1992, and August 1993 and X% of the phones had decals. Decals were applied to all phones without them.

c. All fax cover sheets include the required "consent-to-monitor" warning statement(see Attachment 2).

d. Cellular telephone users are required to sign a receipt that includes the warning "statement of consent to monitor." (see Attachment 3) or the DD Forms 2056 were affixed to the telephones.

e. A banner containing the consent warning statement has been installed on all computers. This statement is automatically displayed on computer monitors upon logon.

f. Six Daily Bulletin items were published and one article in the Base Newspaper publicized possible monitoring (see Attachment 3).

g. The installation commander published the attached letters to all personnel advising them that the telecommunications are subject to monitoring (see Attachment 2).

h. A sticker has been attached to all data modems, facsimile machines, and computer monitors. The sticker states: THIS TELECOMMUNICATIONS DEVICE IS SUBJECT TO MONITORING AT ALL TIMES. USING THIS DEVICE CONSTITUTES CONSENT TO MONITORING.

i. Other notification actions: OPR briefed four commander's calls and two wing staff meetings.

JOE DEANGELO, Lt Col, USAF

Commander

5 Attachments:

1. Advisement Letters
2. In-Processing Briefing
3. Bulletins and Article
4. Fax Cover Sheet
5. Cellular Phone Notification Form

1st Ind, JA 12 Jun 95

TO: 123 COMMUNICATIONS SQUADRON

In accordance with AFI 33-219, I have determined that the notification actions outlined in your summary letter are legally ample to provide sufficient notice to base personnel that using DoD telecommunications constitutes consent to telecommunications monitoring.

STEPHEN PETERS, Col, USAF

Judge Advocate

Attachment 4

IC 2000-1 TO AFI 33-219, TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM (TMAP), 1 JUNE 1998

15 May 2000

SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2000-1, which replaces **Attachment 1** and paragraph A2.3.5. in **Attachment 2**. The change in **Attachment 2** provides the updated notice and consent log-on banner notification statement.

Attachment 1
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

DoDD 8000.1, *Defense Information Management (IM) Program*

AFPD 10-11, *Operations Security*

AFPD 33-2, *Information Protection*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

AFI 71-101, Volume 2, *Protective Service Matters*

OASD/C3I, *Memorandum, Communications Security (COMSEC) Monitoring*, 14 April 1999

Abbreviations and Acronyms

67IW--67th Intelligence Wing

AFCA--Air Force Communications Agency

AFCIC--Air Force Communications and Information Center

AFI--Air Force Instruction

AFIWC--Air Force Information Warfare Center

AIA--Air Intelligence Agency

AFOSI--Air Force Office of Special Investigations

AFPD--Air Force Policy Directive

ASD--Assistant Secretary of Defense

CI--Critical Information

C3I--Command, Control, Communications, and Intelligence

DoD--Department of Defense

DTS--Defense Telecommunications Service

DV--Distinguished Visitor

IP--Information Protection

JCS--Joint Chiefs of Staff

MAJCOM--Major Command

NCR--National Capital Region

OPFOR--Opposition Forces

OPR--Office of Primary Responsibility

OPSEC--Operations Security

PPI--Personal Privacy Information

RCS--Reports Control Symbol

SAF--Secretary of the Air Force

SJA--Staff Judge Advocate

TMR--Telecommunications Monitoring Report

TAR--Telecommunications Assessment Report

TMAP--Telecommunications Monitoring and Assessment Program

USAF--United States Air Force

Terms

Consumer--Normally the Air Force unit identified to receive support, i.e., the requesting MAJCOM, or a subordinate unit at any level of command.

Critical Information (CI)--Information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage. Such information if released prematurely, may prevent or forestall mission accomplishment, reduce mission effectiveness, or cause loss of lives and/or damage to friendly resources.

Information Systems--a. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual (DoDD 8000.1, *Defense Information Management (IM) Program*). b. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. (AFPD 33-2, *Information Protection*).

Notice and Consent--A notification program that includes all actions taken to make sure users of official DoD telecommunications systems/devices are adequately notified that using official DoD telecommunications systems/devices constitutes consent to telecommunications monitoring.

Open Information Systems--Any information system or activity that is accessed or observed by personnel outside the system and provides information by open sources or OPSEC indicators. Open information systems use open source information to provide OPSEC indicators that may be observed by adversaries.

Open information systems may also be influenced, jammed, interrupted, or exploited by adversaries and adversarial weapons systems. Examples are nonsecured telephone systems, computer systems connected to outside lines, and unsecured radio systems.

Personal Privacy Information (PPI)--Any item, collection or grouping of information about an individual's private or personal affairs, including (but not limited to) personal financial matters, social behavior, medical conditions, or any other information, the release of which would be considered an unwarranted invasion of the individual’s privacy.

Requeste--Normally a MAJCOM that requests TMAP support. On certain occasions, a requester could be HQ AIA, HQ AIA theater wings, or Air Force operational units down to wing level.

Telecommunications--Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems (JP 1-02).

Telecommunications Assessment--An evaluation of telecommunications to identify, analyze and report inadvertent disclosures of classified/sensitive information.

Transcript--A verbatim typewritten reproduction of a monitored communication including (if contained in the communication) conversants' names, telephone numbers, circuit designators, organizations, call signs, and other identifying data. Any explanatory or other comments included in a transcript are clearly offset and indicated as such so they are not construed as part of the transcribed communication. The following terms also apply to transcripts:

Sanitized Transcript--A transcript that was edited to remove the names of conversants and any other data that could reasonably identify conversants.

Unsanitized Transcript--A term that means the same as transcript. It is used when needed to clearly discriminate between transcript and sanitized transcript.

Unsecured Telecommunications--Telecommunications which do not use authorized cryptographic products or protected distribution systems.

Addresses

67 IW/CC

248 Kirknewton St

San Antonio TX 78243-7150

HQ AFCA/ITPP

203 West Losey Street, Room 1060

Scott AFB IL 62225-5232

HQ AFCIC/SYN

1250 Air Force Pentagon, Room 4A1088E

Washington DC 20330-1250

HQ AIA/DO

102 Hall Blvd, Suite 229

Kelly AFB TX 78243-7029

HQ USAF/XOO

1630 Air Force Pentagon, Room 4E1046

Washington DC 20330-1630

SAF/GC

1740 Air Force Pentagon, Room 4E856

Washington DC 20330-1740

Attachment 2
NOTICE AND CONSENT PROCEDURES

A2.3.5. Put users of Air Force computer systems on notice that system use constitutes consent to monitoring and system testing. Install a notice and consent log-on banner on all computers. At the minimum, proper notification in terms of content is:

"This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes."