

1 MAY 2006



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://www.e-publishing.af.mil>

OPR: HQ AIA/DO (Col Ronald Haygood)

Certified by: SAF/XCIA
(Col Gary W. Klabunde)

Supersedes AFI 33-219, 23 May 2002

Pages: 42

Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and prescribes responsibilities, procedures, and guidance concerning the Telecommunications Monitoring and Assessment Program (TMAP). It also implements national and Department of Defense (DOD) directives pertaining to the monitoring of unsecured telecommunications for information content and establishes a requirement for feedback in the operations security (OPSEC) process AFPD 10-11, *Operations Security* (will be superseded by AFPD 10-7, *Information Operations*). Guidance in Air Force Instruction (AFI) 71-101, Volume 2, *Protective Service Matters*, concerning telephone interception and eavesdropping does not apply to telecommunications monitoring conducted according to this instruction. AFPD 10-20, *Air Force Defensive Counterinformation Operations* (will be superseded by AFPD 10-7), requires OPSEC participation as part of its employment capabilities for Defensive Counterinformation (DCI) operations to protect and defend DOD/Air Force information and information systems. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by the DOD that operate information systems. Certain aspects of this instruction apply to all users of Air Force-controlled DOD telecommunications systems, equipment, and devices. This instruction applies to the Air National Guard (ANG). Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, provides more current background for OPSEC relationships. Find additional security instructions and manuals on the Air Force Publishing Web Site at <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. **Failure to observe the prohibitions and mandatory provisions of this instruction in paragraphs 21.8. and 21.9. by military personnel is a violation of Article 92, Uniform Code of Military Justice. Violations by civilian employees may result in administrative or disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.** Direct questions or comments on the content of this instruction to Headquarters Air Intelligence Agency (HQ AIA/DO), 102 Hall Blvd, Suite 115A, San Antonio TX 78243-7029. Refer suggested changes or conflicts between this and other instructions through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/EASD), 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force (AF) IMT 847, **Recommendation for**

Change of Publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363) and disposed of in accordance with Air Force Records Information Management System (AFRIMS), *Records Disposition Schedule (RDS)* located at https://afrims.amc.af.mil/rds_series.cfm. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change incorporates interim change IC 2006-1 (Attachment 5). It updates organization names, office symbols and references. This change adds responsibilities for the commanders of Air Combat Command (ACC) (paragraph 7.1), Eighth Air Force (paragraph 7.2) and the 67th Information Operations Wing (paragraph 7.3). It properly aligns oversight and focal point responsibility for monitoring telecommunications systems to HQ USAF/A3I (paragraph 7). This change clarifies the notice and consent requirement for private/intranet unit homepages (paragraph 13.8.3 and A3.3.6.3). It updates the title of Section D, clarifies the annual TMAP assessment requirements in paragraphs 17 and the tasking priorities in 17.2, adds tasking priorities for HQ AIA/DO (paragraph 17.3) and removes guidance on out-of-cycle TMAP requests (paragraph 19). This change identifies the proper coordination channels on the use of TMAP information for law enforcement and adverse actions (paragraph 25). Paragraph 27.2 was updated to reflect the AFRIMS website. Additionally, the mandatory notice and consent procedures in Attachment 3 were clarified to include the requirements for Personal Electronic Devices (paragraph A3.3.4), expanded examples of computer systems (paragraph A3.3.6), expanded guidance for computer system log-on banners (paragraph A3.3.6.1), requirements for systems with financial or technical limitations to the log-on banner installation (paragraph A3.3.6.2), and requirements for private/intranet unit homepages (paragraph A3.3.6.3). The example in Attachment 4 was updated to reflect the clarified guidance in Attachment 3. A bar (|) indicates a revision from the previous edition.

Section A—Telecommunications Monitoring and Assessment Program (TMAP)	5
1. Telecommunications.	5
2. Telecommunications Monitoring and Assessment Program Assessments.	5
3. Telecommunications Monitoring and Assessment Program Reports.	5
4. Telecommunications Monitoring and Assessment Program Authority.	5
Section B—Responsibilities	5
5. The Assistant Secretary of Defense/Networks and Information Integration (ASD/NII).	5
6. The Secretary of the Air Force, General Counsel (SAF/GC).	6
7. HQ USAF/A3I.	6
8. Secretary of the Air Force, Information, Services and Integration Directorate, Information Assurance Division (SAF/XCIA).	6
9. Headquarters Air Force Communications Agency (HQ AFCA).	6
10. HQ AIA/DO.	6
11. MAJCOM, FOA, and DRU Information Assurance (IA) Offices.	7

12.	MAJCOM, FOA, and DRU OPSEC Offices.	7
13.	Base/Facilities/Organizations.	7
Section C—Notice and Consent Procedures		9
14.	General Notification.	9
15.	Performing Telecommunications Monitoring and Assessment Program Functions.	9
16.	Notice and Consent Certification Process.	9
Table 1.	TMAP Certification Schedule.	11
Section D—Obtaining Telecommunications Monitoring Assessments		11
17.	Identifying Monitoring Requirements.	11
18.	Joint Chiefs of Staff Support.	12
19.	DELETED	12
20.	Threat Consideration.	12
Section E—Telecommunications Monitoring and Assessment Program Procedures		13
21.	HQ AIA Telecommunications Monitoring and Assessment Program Personnel Will:	13
Section F—Telecommunications Monitoring and Assessment Program Reports		13
22.	HQ AIA Telecommunications Monitoring and Assessment Program Reports.	13
Section G—Using and Controlling Telecommunications Monitoring and Assessment Program Information		14
23.	Uses and Restrictions.	14
24.	Requesting and Releasing Telecommunications Monitoring and Assessment Program Information and Transcripts.	15
25.	Using Telecommunications Monitoring and Assessment Program (TMAP) Information for Law Enforcement and Adverse Actions.	17
Section H—Releasing Telecommunications Monitoring and Assessment Program Information to Enhance OPSEC Awareness and Education		17
26.	Supporting Operations Security Awareness, Training, and Education.	17
27.	Information Collections, Records, and Forms.	17

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	18
Attachment 2— SECURITY CLASSIFICATION GUIDANCE FOR TMAP REPORTS	22
Attachment 3— NOTICE AND CONSENT PROCEDURES	23
Attachment 4— EXAMPLE OF NOTICE AND CONSENT MEMORANDUM AND 1ST IND	26
Attachment 5— IC 2006-1 TO AFI 33-219, TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM (TMAP)	28

Section A—Telecommunications Monitoring and Assessment Program (TMAP)

1. Telecommunications. The Air Force uses unsecured telecommunications systems such as telephones, cellular phones, radios, facsimile, pagers, computer networks, and other wired or wireless electronic devices 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 Assessments. The Air Force monitors unsecured and unprotected telecommunications systems to determine if they are being used to transmit sensitive or classified information. Information collected is analyzed to determine if any sensitive or classified information transmitted on unsecured and unprotected systems could adversely affect United States (U.S.) (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, FOAs, and DRUs as long-term information liabilities. The Air Force conducts TMAP assessments on a continuous basis with monitoring resources adjusted 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 weapons system, operation, or activity, and document their vulnerability to hostile signal intelligence exploitation. Through systematic data assessment and analytical procedures, TMAP teams document the threat, isolate existing or potential OPSEC vulnerabilities; and identify procedures to minimize or eliminate OPSEC vulnerabilities. TMAP is an integral part of the United States Air Force (USAF) OPSEC, Information Operations (IO) Red Teaming, and DCI programs. It is a very effective tool to identify real world problems that can adversely affect the warfighter's effectiveness. During assessments, items such as stereotyped patterns or administrative and physical security procedures routinely surface as possible sources of intelligence losses. 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 U.S. (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/Networks and Information Integration (ASD/NII). 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 provides 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. The requesting unit provides information copies to Headquarters United States Air Force (HQ USAF/A3I), 1630 Air Force Pentagon, Room 4E1046, Washington DC 20330-1630. HQ AIA/DO reviews the request as soon as possible, and if capable of supporting the request, pursues the ASD/NII 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 3](#). This office authorizes initiation or continuation of TMAP monitoring at installations that provide legally adequate notice to users of DoD telecommunications systems, equipment, and devices that such use constitutes consent to TMAP monitoring.

7. HQ USAF/A3I. Provides oversight, advocacy and acts as the focal point for TMAP according to AFI 10-701, *Operations Security*.

7.1. Commander, Air Combat Command (ACC):

7.1.1. Provide TMAP operations in support of OPSEC assessment capabilities for the Air Force.

7.1.2. Coordinate with the Joint Staff, the National Security Agency, or other DoD components for monitoring telecommunications systems that carry both Air Force and other government agency information.

7.2. Commander, Eighth Air Force (8 AF/CC). Designated by the Chief of Staff of the Air Force as the overall tasking authority for TMAP operations to be conducted at any time on any Air Force installation certified by SAF/GC as compliant with established notice and consent procedures.

7.3. Commander, 67th Information Operations Wing (67 IOW). Delegated by the 8 AF/CC to be the operational tasking authority (see paragraph 17) for TMAP operations to be conducted at any time on any Air Force installation certified by SAF/GC as compliant with established notice and consent procedures.

8. Secretary of the Air Force, Information, Services and Integration Directorate, Information Assurance Division (SAF/XCIA). This is the lead office within the Air Force for policy matters affecting notice and consent certification and related issues.

9. Headquarters Air Force Communications Agency (HQ AFCA).

9.1. HQ AFCA/EVP notifies the MAJCOM, FOA, and DRU Information Assurance (IA) offices in early February during even-numbered fiscal years to initiate biennial notification procedures.

9.2. HQ AFCA/EVP acts as the focal point for the notice and consent certification process.

9.3. HQ AFCA/JA acts as the focal point for reviewing the summaries and Staff Judge Advocate (SJA) determinations. This office endorses the report prior to sending it to SAF/GC for certification.

10. HQ AIA/DO.

10.1. Organizes and trains combat ready forces to provide combatant commanders with TMAP capabilities.

- 10.2. Develops, funds, procures, and maintains modern TMAP capabilities to support current and future USAF operations.
- 10.3. Provide TMAP resources to assist MAJCOMs, FOAs and DRUs and subordinate organizations assess communications vulnerabilities.
- 10.4. 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.
- 10.5. Coordinates with HQ AFCA to obtain biennial notice and consent determinations.
- 10.6. Interacts with IO Red Teaming activities to assess and evaluate the defensive readiness of Air Force units and identify friendly OPSEC weaknesses that may impact effectiveness of military operations. Provides TMAP products to IO Red Teaming/DCI Fusion Center according to AFPD 10-20 and associated AFIs.
- 10.7. Integrates TMAP assessments into Air Force-wide OPSEC programs.
- 10.8. Maintains awareness of changing threats to friendly telecommunications and informs supported Air Force activities of trends and potentially dangerous situations.
- 10.9. Performs TMAP activities only at installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

11. MAJCOM, FOA, and DRU Information Assurance (IA) Offices.

- 11.1. Assess base compliance with this instruction during IA Assessment Team visits.
- 11.2. Ensure base/facility notification and consent actions comply with [Section C](#) and [Attachment 3](#).
- 11.3. Include TMAP assessments in appropriate operations and exercise plans.
- 11.4. Request TMAP assessments from HQ AIA according to [Section D](#).
- 11.5. Include separate endorsement on each base package.
- 11.6. Maintain documentation (Attachments 1 through 6 of example) in Attachment 4 of this AFI, at MAJCOM, FOA, and DRU-level.
- 11.7. The FOAs and DRUs located on a host base will report through the wing/IA office.
- 11.8. The FOAs and DRUs not located on a host base will report as a wing/IA office.

12. MAJCOM, FOA, and DRU OPSEC Offices.

- 12.1. 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.”
- 12.2. Include TMAP assessments in appropriate operations and exercise plans.
- 12.3. Coordinate TMAP assessments from HQ AIA according to [Section D](#).

13. Base/Facilities/Organizations.

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

13.2. Installation officials must educate their personnel that the DoD frequently transmits information via radio, which makes the information readily susceptible to interception and analysis by our adversaries.

13.3. Establish and accomplish notice and consent procedures according to [Section C](#) and [Attachment 3](#).

13.4. Send annual requests for TMAP assessments to their respective MAJCOMs, FOAs and DRUs.

13.5. Include TMAP assessments in appropriate operations and exercise plans.

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

13.6.1. Stay familiar with the operation under study.

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

13.6.3. Keep familiar with TMAP objectives and methods.

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

13.6.5. Help the TMAP team in determining proper classification of report content and report classification authority when required (see [Attachment 2](#)).

13.6.6. Provide necessary technical information when requested (e.g., frequencies, system specifications, circuit listings, and critical nodes).

13.6.7. 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.

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

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

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

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

13.6.12. Give TMAP personnel access to operational orders and plans, operating instructions, security classification guides, 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.

13.7. Wing IA Offices.

13.7.1. Compile unit reports into one summary report for the installation. Ensure facilities not on the installation and geographically separated units are specified in the summary letter.

13.7.2. Ensure compliance with notice and consent requirements by annually checking Wing information systems subject to monitoring according to AFI 33-230, *Information Assurance Assessment and Assistance Program*.

13.7.3. Make sure the base telephone book complies with paragraph [A3.3.1](#).

13.7.4. Biennially compile the summary letter based on the unit annual reports and submit to the Wing commander for signature. Obtain installation SJA endorsement to the summary letter and send to the MAJCOM, FOA, and DRU IA office.

13.8. Units:

13.8.1. Appoint a TMAP point of contact (POC) to ensure compliance with the applicable requirements of this instruction. This applies to all units that receive support by the host communications unit for any telecommunication systems, to include, but not limited to telephones, facsimile machines, automated information systems, networks, cellular telephones, and hand-held radios. Send a current copy of the unit TMAP POC appointment letter to the Wing IA office.

13.8.2. Quarterly spot-check all telecommunications systems to ensure compliance with [Attachment 3](#).

13.8.3. Ensure the **first pages** on all the unit's private/intranet web homepages comply with [Attachment 3](#). (NOTE: Notice and consent requirements do not apply to public web sites/pages. See AFI 33-129, *Web Management and Internet Use*, for Privacy and Security Notice requirements for public web sites/pages.)

13.8.4. Submit a biennial report to the Wing IA office according to [Attachment 4](#).

13.9. Air National Guard. When the guard is a tenant unit on an installation, they submit their TMAP package to the supporting Wing IA office. If they are on their own installation, they submit their package to the National Guard Bureau.

13.10. Non-compliance. Subordinate organizations must report corrective actions back to the Wing IA office within 30 days. If the organization does not report compliance within thirty days, affected communications services may be suspended by the installation commander or his/her delegee.

Section C—Notice and Consent Procedures

14. General Notification. Provide general notification of monitoring activity to all users of DoD telecommunications systems and devices to ensure they are aware and consent to telecommunications monitoring.

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

16. Notice and Consent Certification Process.

16.1. Wing IA Office. The Wing IA office 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 notice and consent actions following procedures described in [Attachment 3](#). The Wing IA office sends this summary through the installation SJA to the installation/Wing commander by 15 April of each even-numbered fiscal year. Summaries covering more than one installation must clearly identify each installation. The description of each notification action must indicate how the action applies to each installation. As a minimum, complete and document the actions out-

lined in [Attachment 3](#). An example of a summary letter is in [Attachment 4](#). Upon receipt of the SJA endorsement, the Wing IA office sends it, along with the base summary, to their MAJCOM IA office NO LATER THAN 1 MAY.

16.2. Installation Staff Judge Advocates. The installation SJA reviews the summary and attached documentation and provides written review (see [Attachment 4](#) for suggested SJA 1st Ind format). This SJA review should ensure the actions taken are sufficient to establish compliance with the requirements of this instruction. In particular, the summary and its attachments should clearly demonstrate that users of DoD telecommunications equipment know that such use constitutes consent to telecommunications monitoring. If the SJA determines the documentation is deficient in any of the requirements, the package should be returned for corrective action. If the package is determined to be legally sufficient, the Wing IA office includes the SJA's written determination as part of the TMAP certification package.

16.3. MAJCOM, FOA, and DRU IA Offices. These offices ensure all subordinate bases and installations under their control respond in a timely manner and that the information provided in the package complies with the requirements of this instruction. The MAJCOM, FOA, and DRU IA offices send the completed summary report and documentation to the MAJCOM, FOA, and DRU SJA for review. Following this legal review (and correction of any deficiencies noted), the MAJCOM, FOA, and DRU IA offices send the summary report and SJA determination to HQ AFCA/EVP, 203 W. Losey, Room 2200, Scott AFB IL 62225-5222. Submit these reports by 15 May of each even-numbered year.

16.4. HQ AFCA/EVP. This office ensures all USAF facilities submit inputs in order to receive biennial SAF/GC certification. This office sends all summaries and SJA determinations to HQ AFCA/JA for review and endorsement. TMAP files containing insufficient evidence of monitoring notice and consent as required by this instruction are returned to the appropriate MAJCOM IA offices for follow-on corrective action. HQ AFCA/EVP sends all summaries of actions to SAF/GC, 1740 Air Force Pentagon, Room 4E856, Washington, DC 20330-1740, by 15 July each even-numbered fiscal year.

16.5. SAF/GC. Certifies sufficient notice of TMAP monitoring is provided to users of DOD telecommunications systems of specific USAF installations and authorizes use of TMAP assessments at approved installations. If the General Counsel determines the base summary report contains insufficient evidence to establish full compliance with notice of monitoring requirements, the summary is returned for further corrective action prior to certification. This office returns a certification listing to HQ AFCA/EVP by 1 September of each even-numbered fiscal year, listing installations approved to receive TMAP assessments. This certification listing is valid for 2 years expiring on 30 September.

16.6. HQ AFCA sends any deficiencies noted by SAF/GC to HQ AIA/DO and MAJCOM, FOA, and DRU IA offices. HQ AFCA works with the MAJCOM, FOA, and DRU IA offices to ensure that installations not certified by SAF/GC meet the notice and consent requirements, accomplish whatever actions are determined incomplete or deficient, and resubmits the summary packages for SAF/GC reevaluation and approval.

16.7. 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.

16.8. The TMAP date notification schedule of events for certification is in [Table 1](#).

Table 1. TMAP Certification Schedule.

Even Year Date	Office	Action
Early Feb	HQ AFCA/EVP	Initiates Biennial notification procedures
15 Feb – 15 Apr	Wing IA Office	Prepares Summary
15 Apr	Wing IA Office	Sends Summary to Base SJA
1 May	MAJCOM, FOA, and DRU IA Office	Reviews Summary and MAJCOM, FOA, and DRU SJA Review
15 May	MAJCOM, FOA, and DRU IA Office	Sends Summary to HQ AFCA/EVP with MAJCOM, FOA, and DRU SJA endorsement
15 May - 15 Jul	HQ AFCA/EVP	Reviews all Summaries with HQ AFCA/JA
15 Jul	HQ AFCA/EVP	Sends summaries to SAF/GC
1 Sep	SAF/GC	Provides HQ AFCA/EVP with a list of bases approved to continue TMAP monitoring
15 Sep	HQ AFCA/EVP	Releases a message listing certified bases

Section D—Obtaining Telecommunications Monitoring Assessments

17. Identifying Monitoring Requirements. Air Force organizations desiring TMAP/Electronic System Security Assessments (ESSA) support identify their requirements to the 67 IOW's ESSA Tasking Cell (ETC), 67th Operations Support Squadron (OSS), for scheduling and prioritization. Each January, HQ AIA/DO requests all MAJCOMs, FOAs and DRUs provide TMAP assessment requirements based on HQ AIA/67 IOW ESSA program enhancements for the proceeding fiscal year. MAJCOMs, FOAs, and DRUs respond by 15 July of each year with TMAP assessment requests. By 15 September, the 67 IOW tasks HQ AIA TMAP elements based on requests submitted. For customers with an established continuous monitoring tasking, review the tasking document annually by 1 October and update as warranted with current signatories. This tasking document constitutes authority for TMAP elements to operate, if the installations scheduled for monitoring are currently certified by SAF/GC.

17.1. Time Phased Force Deployment Document (TPFDD) events. For contingencies and exercises with a force structure driven by a TPFDD, TMAP assessment requirements should be unit type code driven and tasked to HQ AIA as the sole Air Force “force provider,” in accordance with AFMAN 10-401, Volume 1, *Operation Plan and Concept Plan Development and Implementation*.

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

17.2.1. Priority 1. Contingency operations.

17.2.1.1. 1A. Combat planning cells.

17.2.1.2. 1B. Combat enabling forces.

17.2.1.3. 1C. Military Operations Other than War.

17.2.2. Priority 2. Special Access Programs (SAP) and research, development, test and evaluation (RDT&E) of USAF Emerging Technologies.

17.2.2.1. 2A. Existing SAPs.

17.2.2.2. 2B. Test and Evaluations.

17.2.2.3. 2C. Research and Development.

17.2.3. Priority 3. Air Expeditionary Force predeployment exercises/events.

17.2.4. Priority 4. Joint Chiefs of Staff directed exercise.

17.2.5. Priority 5. Combatant command/MAJCOM exercises.

17.2.6. Priority 6. Baseline assessments.

17.2.7. Priority 7. All other requirements.

17.3. Biannual Requirements and Tasking Priorities. Each September and April, HQ AIA/DO requests Community of Interest (COI) members identify TMAP requirements for scheduled Air Force events/operations (exercises, reoccurring events, baseline OPSEC assessments, etc). The ETC consolidates and prioritizes all scheduled and ad-hoc requirements identified by the COI in accordance with the tasking priority list. The ETC then tasks worldwide TMAP units using an ESSA Tasking Order.

18. Joint Chiefs of Staff Support. JCS policy tasks the military services to furnish telecommunications monitoring support for JCS directed operations and exercises. HQ AIA/DO 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.

18.1. If the Joint Communication Security (COMSEC) Monitoring Activity (JCMA) is designated as Executive Agent for telecommunications monitoring, requests should be levied as a joint requirement to JCMA and executed under the Joint Operations and Planning Execution System in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.03A, *Joint Operations Planning and Execution System, Volume II, Planning Formats and Guidance*, 31 December 1999, C1, 6 September 2000.

18.2. If JCMA is not designated as the Executive Agent for telecommunications monitoring, unified or specified commands coordinate with the ESSA Tasking Cell, through the Air Force component command as a member of the COI. Execute requirements in accordance with AFMAN 10-401.

19. DELETED

20. Threat Consideration. By 1 June of each year, each Electronic System Security Assessment Central (ESSAC) requests threat assessments from Air Force Information Warfare Center (AFIWC/OSA) via the COLISEUM tasking database, based on theater communication infrastructure. By 1 September of each year, the AFIWC evaluates the threat and furnishes data to the appropriate theater ESSAC. The ESSAC 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 Inter-agency Air Force Information Collections*.

Section E—Telecommunications Monitoring and Assessment Program Procedures

21. HQ AIA Telecommunications Monitoring and Assessment Program Personnel Will:

21.1. Comply with applicable Federal laws, National, DoD, and JCS policy, and this instruction. **Failure to observe the prohibitions and mandatory provisions of this instruction in paragraphs 21.8. and 21.9. by military personnel is a violation of Article 92, Uniform Code of Military Justice. Violations by civilian employees may result in administrative or disciplinary action without regard to otherwise 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. Ensure monitoring requests from outside Air Force, Air Force Reserves, or Air National Guard entities are coordinated with the JCMA.

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

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

21.6. Monitor wireless telecommunications only when the monitoring equipment is technically capable of isolating monitoring to specific DoD telecommunication devices. If the equipment utilized cannot clearly and specifically demonstrate this capability, seek a legal review prior to the starting any monitoring operations.

21.7. Do not use tone-warning devices when using recording equipment for TMAP activities.

21.8. Do not intentionally report or file any acquisition or proprietary information, or personal privacy information (PPI) extraneous to the TMAP activity. Information identified as potentially privileged; i.e., confidential communications between attorney and client, husband and wife, or clergy and penitent, may only be reported after consultation with the servicing legal office.

21.9. Promptly destroy any such information 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. Such collected information that is not destroyed shall be reported according to the provisions of paragraph 24.5.

Section F—Telecommunications Monitoring and Assessment Program Reports

22. HQ AIA Telecommunications Monitoring and Assessment Program Reports. When accomplishing TMAP activities in conjunction with Multiple Discipline Vulnerability Assessments (MDVA), include TMAP reports as part of the MDVA report. Basic types of reports are:

22.1. Telecommunications Monitoring Report. A timely, usually brief report, used to notify the consumer of suspected intelligence disclosures. These reports may contain intentional or unintentional compromises of classified information, classified or unclassified information of possible immediate or short-term intelligence value to Hostile Intelligence Services, critical information (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. The reporting requirement in this paragraph is exempt from licensing according to AFI 33-324.

22.3. When operating under the Executive Agency of JCMA the following reports apply:

22.3.1. Tactical Advisory. Provides time-sensitive information force protection information and mission critical information during exercise and real world operations.

22.3.2. Daily Summary. Provides a summary of the COMSEC disclosures and trends in a 24-hour period.

22.3.3. Periodic Analytical Summary. Provides highlights of significant COMSEC trends or vulnerabilities, as required.

22.3.4. Final Analytical Summary. Provides a summary of the results of monitoring upon completion of an operation, exercise, or assessment. Includes vulnerability and threat analysis and recommendations. Disseminated via electronic message or written report.

22.4. Based on evolving information technologies and new DoD mission areas resulting from the development of the National Security Strategies in the information realm, TMAP products may be used in the emergence of new DoD/Air Force entities (e.g., IO Red Teaming and DCI Fusion Center), within restrictions set forth in [Section G](#).

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

23. Uses and Restrictions. Use information in the TMAP reports only for official U.S. government TMAP purposes, except as noted. 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/DO personnel use information developed from monitored telecommunications as the basis for issuing reports to military commanders 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 electronic mail (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 assessments to produce foreign intelligence or counterintelligence information.

23.3. The results of TMAP assessments 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 signal 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 Assessment 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 will 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 e-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 the HQ AIA/DO evaluation determines the release of names and identifying data is justified after receiving advice from HQ AIA/JA, 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 directly to joint or unified command authorities, when reviewed and approved by the joint or unified Judge Advocate Authority or 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 obtained while monitoring Air Force activities. When this occurs, provide the sanitized transcript to HQ AIA/DO for further processing. DoD components requiring sanitized transcripts must send requests to HQ AIA/DO. If the DoD component's review determines unsanitized transcripts are required, procedures set forth in paragraphs [24.1.](#) and [24.2.](#) apply.

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 U.S. weaknesses and capabilities. When a HQ 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 conversations of U.S. personnel are not releasable outside the allied telecommunications monitor cell without HQ AIA/DO approval as outlined above.

24.5. Information acquired during the course of an authorized TMAP operation that reveals an emergency situation threatening death or grievous bodily harm and/or major loss of property must be immediately reported to the military commander, the Air Force Office of Special Investigations (AFOSI), or the U.S. law enforcement agency having jurisdiction. Use the most expeditious means available that provides adequate security. Full identifying data may be released. This is not a TMAP report. Immediate action may be taken by the responsible military commander or law enforcement agency to address the emergency situation.

24.5.1. Information acquired during the course of an authorized TMAP operation that relates directly to a significant crime (or significant fraud, waste, or abuse) must be reported (except privileged communications, see paragraph 21.8.) to the military commander with court-martial convening authority, AFOSI, or law enforcement agency having jurisdiction over the unit being monitored. Full identifying data may be released. This is not a TMAP report.

24.5.2. Within 24 hours of initial notification under paragraphs 24.5. and 24.5.1., notify HQ AIA/DO/JA, by message, with copies to 67 IOW/CC, 467 Moore St., San Antonio, TX 78243-7135.

24.5.3. Information acquired during the course of a TMAP operation that reveals a compromise or continuing threat of compromise of classified national security information must be immediately reported to the appropriate network control officials. If classified information is recovered during the course of an e-mail monitor mission, the mission supervisor or designated representative is authorized to release enough identifying data to the appropriate network control officials to facilitate the containment and remediation of the compromised data. Release the minimum amount of data necessary to ensure prompt remedial action. Reporting of the incident will be for the sole purpose of minimizing exposure of national security information to unauthorized personnel.

24.5.4. Commanders must follow the procedures contained in paragraph 25. prior to taking administrative or disciplinary action based on TMAP materials.

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, General officers, 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 U.S. 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 (TMAP) Information for Law Enforcement and Adverse Actions. Information acquired during the course of an authorized TMAP operation that is provided to Air Force officials pursuant to paragraph 24.5, may not be used for adverse administrative or disciplinary actions against an individual identified through such TMAP information without submitting the matter through HQ AIA/DO/JA to HQ USAF/A3II and SAF/GC. Information obtained during TMAP operations may not be used for adverse administrative or disciplinary actions without the approval of SAF/GC.

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

26. Supporting Operations Security Awareness, Training, and Education. Improving operations security within the Air Force depends in large part 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 information for use in the Air Force OPSEC program. AFIWC/OS provides information for educational purposes in response to a specific request, or the HQ AIA/DO 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. If extracted communications from outside the requesting organization are required to meet a consumer's need, the extracts will not identify the base or organization involved in the monitored telecommunications.

27. Information Collections, Records, and Forms.

27.1. Information Collections: RCS: HAF SC(BE)9497, **Summary of Consent Notification Actions**, is mandated by this publication. See paragraph 16.1. for guidance. Other information collections identified in this publication are exempt from licensing according to AFI 33-324.

27.2. Records: Maintain and dispose of records created by this publication in accordance with AFRIMS RDS, Table 33-24, Rule 1, 5, 7, 8, and 9, is located at https://afrims.amc.af.mil/rds_series.cfm.

27.3. Forms (Adopted and Prescribed).

27.3.1. Adopted Forms. AF Form 847, AF Form 3535, and DD Form 2056.

27.3.2. Prescribed Forms. No forms are prescribed by this publication.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and Chief Information Officer

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

CJCSM 3122.03A, *Joint Operations Planning and Execution System, Volume II, Planning Formats and Guidance*, 31 December 1999, C1, 6 September 2000

Paperwork Reduction Act of 1995

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

DODD 4640.6, *Communications Security Telephone Monitoring and Recording*, 26 June 1981 (Note: to be superseded by DODD 8560.aa)

DODM 4525.8-M, AF Sup 1, *Official Mail Manual*

AFDD 2-5, *Information Operations*

AFPD 10-11, *Operations Security* (will be superseded by AFPD 10-7, *Information Operations*)

AFPD 10-20, *Air Force Defensive Counterinformation Operations* (will be superseded by AFPD 10-7, *Information Operations*)

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

AFI 10-701, *Operations Security*

AFI 33-129, *Web Management and Internet Use*

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

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*

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

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

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

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

Abbreviations and Acronyms

8th AF—Eighth Air Force

67 IOW—67th Information Operations Wing

67 OSS—67th Operations Support Squadron

AF—Air Force (when used on forms)

AFCA—Air Force Communications Agency

AFDD—Air Force doctrine document

AFDIR—Air Force Directory
AFI—Air Force Instruction
AFIWC—Air Force Information Warfare Center
AFMAN—Air Force manual
AFOSI—Air Force Office of Special Investigations
AFPD—Air Force policy directive
AFRIMS—Air Force Records Information Management System
AIA—Air Intelligence Agency
ANG—Air National Guard
ASD—Assistant Secretary of Defense
CI—critical information
CJCSM—Chairman of the Joint Chiefs of Staff manual
COI—community of interest
COMSEC—communications security
DCI—Defensive Counterinformation Operations
DOD—Department of Defense
DRU—direct reporting unit
DTS-W—Defense Telecommunications Service-Washington
DV—distinguished visitor
E-mail—electronic mail
ESSA—electronic system security assessment
ESSAC—Electronic System Security Assessment Central
ETC—ESSA tasking cell
FOA—field operating agency
IO—Information operations
IA—Information assurance
JCMA—Joint COMSEC Monitoring Activity
JCS—Joint Chiefs of Staff
LMR—land mobile radio
MAJCOM—major command
MDVA—multiple discipline vulnerability assessment
NCR—National Capital Region

NII—network and information integrity

OPFOR—opposition forces

OPR—office of primary responsibility

OPSEC—operations security

PED—portable electronic device

POC—point of contact

PPI—personal privacy information

RCS—Reports Control Symbol

RDS—Records Disposition Schedule

RDT&E—Research, Development, Test and Evaluation

SAF—Secretary of the Air Force

SAP—Special Access Program

SJA—Staff Judge Advocate

TAR—Telecommunications Assessment Report

TMAP—Telecommunications Monitoring and Assessment Program

TPFDD—Time Phased Force Deployment Document

U.S.—United States

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 Content—When used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. It does not include communication routing information including Internet Protocol addresses or machine-readable binary packets in a packet switched network used to direct or route the communication.

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

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.

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, FOA, and DRU 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, callsigns, 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.

Unprotected Telecommunications—Telecommunications that do not use authorized unclassified Public Key Encryption products.

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 that does not use authorized cryptographic products or protected distribution systems.

Attachment 2

SECURITY CLASSIFICATION GUIDANCE FOR TMAP REPORTS

A2.1. Security Guidance for Reporting Mission Results. This is minimum-security guidance for reporting. Every effort should be made to obtain Classification Guidance from the unit and/or event being monitored inclusive of Operations Plans, Exercise Plans, Essential Elements of Friendly Information, CI, or Security Classification Guides.

Table A2.1. Security Guidance for Reporting Mission Results.

If the report contains information on:	Which Reveal:	Then the report will be a minimum of:
Sources requiring protection at the secret level	Units in vulnerable locations or involved in sensitive operations	SECRET
Operations more than 48 hours prior to execution	Detailed planning information making the operation vulnerable to foreign hostile exploitation	CONFIDENTIAL
Detailed U.S. or allied military capabilities or intentions	U.S. military vulnerability	CONFIDENTIAL
Events as they occur or post occurrence	U.S. or allied military intentions	FOR OFFICIAL USE ONLY

Attachment 3

NOTICE AND CONSENT PROCEDURES

- A3.1.** Educate personnel about the hostile signal intelligence threat to unsecured telecommunications.
- A3.2.** Provide guidance to users in the proper use of unsecured telecommunications.
- A3.3.** Notify users of DOD telecommunications devices, including contractors and their employees, that using DOD telecommunications systems constitutes consent to telecommunications monitoring. The following notification procedures are ***mandatory*** for official DOD telecommunications systems/devices:

A3.3.1. Installation telephone directories. Prominently display the following notice and consent statement on the front cover of telephone directories, or, if the telephone directory is embedded in a base information guide this notice must precede the telephone directory portion of the base guide: **“DO NOT DISCUSS CLASSIFIED INFORMATION ON UNSECURE TELEPHONES. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES.”** **“DOD telephones are provided for the transmission of official government information only and are subject to communications security monitoring at all times. Use of official DOD telephones constitutes consent to communications security telephone monitoring in accordance with DOD Directive 4640.6.”** This banner is also required on the top of the first page of the electronic version of the telephone directory.

A3.3.2. Telephones.

A3.3.2.1. Affix DD Form 2056, **Telephone Monitoring Notification Decal**, on the front of all official telephones.

A3.3.2.2. For telephones with secure voice capability that can be used in the unsecure mode, such as Secure Telephone Unit, Secure Terminal Equipment, etc., remove the words **“DO NOT DISCUSS CLASSIFIED INFORMATION”** from the form.

A3.3.3. Facsimile Machines. Both of the following actions are required to notify users of facsimile machines:

A3.3.3.1. DODM 4525.8-M, AF Sup 1, *Official Mail Manual*, mandates the use of AF IMT 3535, **Facsimile Electro Mail Transmittal**, when a cover sheet is required for fax transmission. The AF IMT 3535 contains the proper notice and consent statement. If any other cover sheet is used, the following notice and consent statement must be printed on it: **“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.”**

A3.3.3.2. Affix the DD Form 2056, on all facsimile machines.

A3.3.4. Portable Electronic Devices (PED) (e.g., text pagers, personal digital assistants, and cellular telephones) must meet one or both of the following requirements.

A3.3.4.1. When issued the device, require personnel to sign a form that includes the following notice and consent statement: **“Do not transmit classified information over unsecured telecommunications systems. Official DOD telecommunications systems are subject to monitor-**

ing. Using this telecommunications system or device constitutes consent to monitoring.”

The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.3.4.2. Affix the DD Form 2056 on all PEDs.

A3.3.5. Hand-held radios/land mobile radios (LMR) must meet one or both of the following requirements.

A3.3.5.1. Affix the DD Form 2056 on all hand-held radios/LMRs or:

A3.3.5.2. Sign a form that includes the statement in A3.3.4.1. The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.3.6. Put users of official computer systems (includes but is not limited to computers connected to a network, servers, stand-alone computers, portable computers, routers) and private/intranet web pages on notice their use constitutes consent to monitoring as specified in the notice and consent log-on banner cited below.

“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.”

A3.3.6.1. Install the notice and consent log-on banner on all computers. The banner is automatically displayed upon boot-up and/or initial log-on for the computer system regardless of the access methodology (physical, network, remote access, dial-in, etc.). Place the banner on the computers in such a way that the user must press a key to get beyond it, thereby demonstrating acceptance of its provisions.

A3.3.6.2. For systems where it is not cost effective or technically feasible to install the complete notice and consent log-on banner cited above, as determined by the MAJCOM/A6, perform at least two of the following requirements:

A3.3.6.2.1. Affix the notice and consent warning banner (DD Form 2056) on all computer monitors or video display screens of those systems.

A3.3.6.2.2. Users of the system (regardless of access methodology) must sign a receipt statement including the following statement: **This is a Department of Defense system. This system is for authorized U.S. Government use only. This system is subject to monitoring at**

all times. Using this system constitutes consent to monitoring. The signed forms will be retained by the office managing the system until 6 months after the user no longer requires access to the system.

A3.3.6.2.3. Install the following, abbreviated log-on banner on the system: **“This is a Department of Defense system. This system is for authorized U.S. Government use only. This system is subject to monitoring at all times. Using this system constitutes consent to monitoring.”** Use of this option may be appropriate for systems with technical limitations on the amount of text used for initial login notices.

A3.3.6.3. Private/intranet Web Homepages. Prominently display the notice and consent banner on the first pages of ALL the unit’s private/intranet web homepages.

A3.3.7. Any telecommunications devices not otherwise referenced in this attachment must have a DD Form 2056 affixed or the person to whom the device is issued must sign a receipt statement including the following statement: **“This telecommunications device is subject to monitoring at all times. Using this device constitutes consent to monitoring.”** The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.4. Optional methods to get this information to Air Force personnel are:

A3.4.1. Correspondence from the base or facility commander, addressing proper use of unsecured telecommunications, to all assigned units for dissemination to unit personnel.

A3.4.2. Addressing telecommunications issues to newcomers during in-processing, periodic OPSEC awareness briefings, and commander’s calls.

A3.4.3. Using base bulletins, base newspapers, E-mails, web pages, and similar publications on a periodic basis.

A3.4.4. Incorporating notice and consent comments in operating procedures, instructions, etc., that are periodically reviewed by users.

A3.4.5. 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 4**EXAMPLE OF NOTICE AND CONSENT MEMORANDUM AND 1ST IND**

MEMORANDUM FOR: Supporting Legal Office

FROM: XX COMMUNICATIONS SQUADRON

Anywhere AFB 12345

SUBJECT: Summary of Consent Notification Actions Taken During the Two-Year Period From 1 Apr XX - 31 Mar XX (RCS: HAF-SC(BE)9497)

The following actions were taken during the past 2 years to notify users of DOD telecommunications devices that using the telecommunications devices constitutes consent to telecommunications monitoring for Anywhere AFB (and the following Geographically Separated Units: [list]).

- a. The current base telephone directory, dated _____, includes the notice and consent statement on the front cover, or on first page of the official portion of the phone book, in accordance with AFI 33-219 (version date), paragraph A3.3.1 (see Attachment 1). An electronic version of the telephone directory is available on the base Intranet and the notice and consent statement is on the top of the first page (see Attachment 2). **NOTE:** If your base does not have a hard copy phone directory or an electronic phone directory state so in this paragraph.
- b. All telephones were inspected on (date) and __% of all phones had the DD Form 2056 attached. Decals were immediately applied to all non-compliant telephones. Consequently, all telephones have DD Form 2056 affixed as of the date of this report.
- c. All faxes were inspected on (date) and __% of all machines have the DD Form 2056 affixed. Decals were immediately applied to all non-compliant fax machines. Consequently, all faxes have DD Form 2056 affixed as of the date of this report. Use either AF IMT 3535 or another cover sheet that includes the statement in AFI 33-219 (version date), paragraph A3.3.3.1. A sample of a fax cover sheet is attached (see Attachment 3). **NOTE:** Do not submit a copy of AF IMT 3535.
- d. On (date) it was verified that all individuals issued an official portable electronic device (including but not limited to cell phone, text pager, and personal digital assistants) had the DD Form 2056 affixed to the device and/or signed a receipt that includes the notice and consent statement contained in AFI 33-219 (version date), paragraph A3.3.4.1 (see Attachment 4).
- e. All LMRs were inspected on (date) and __% of all instruments had the DD Form 2056 affixed, or it was verified that all individuals issued an LMR/hand-held radio have signed a receipt that includes the notice and consent statement contained in AFI 33-219 (version date), paragraph A3.3.4.1 (see Attachment 4). Decals were immediately affixed to all non-compliant LMRs. Consequently all LMRs have DD Form 2056 affixed or all users have signed the required receipt notice. A sample of letter/receipt for all devices is attached.
- f. The notice and consent banner, in accordance with AFI 33-219 (version date), paragraph A3.3.6., has been installed on all computer systems (including but not limited to computers connected to a network, servers, stand-alone computers, portable computers and routers). The banner is automatically displayed upon boot-up and/or initial log-on for the computer system regardless of the method accessed (see Attachment 5). All computers were inspected and __% of all computers

displayed the log-on banner. The banner was immediately installed on all non-compliant computers. Consequently, all computers display the log-on as of the date of this report.

- g. The current notice and consent banner is prominently displayed on the first pages of ALL of the unit's private/intranet web homepages. The warning banner is worded exactly as the log-on banner shown in AFI 33-219 (version date), paragraph A3.3.6. A print screen copy of the web page is attached (see Attachment 6).
- h. TMAP training was provided to all unit/squadron personnel. This training requirement will be part of the initial and recurring OPSEC training.
- i. Other notification actions: (List any optional methods (AFI 33-219, paragraph A3.4) used to notify unit/squadron personnel.)

JOE DOE, Lt Col, USAF

Commander

6 Attachments

1. Telephone Directory Cover**
2. Print Screen of Electronic Telephone Directory Web Page**
3. Copy locally produced FAX cover sheet, if used**(must have the notice and consent statement on it)
4. Portable Electronic Device Notification Form/LMR**
5. Print Screen of Computer Banner**
6. Print Screen of Unit Private Web Pages with Banner**

**Mandatory attachment

1st Ind, JA 12 Apr 00

TO: 123d Communications Squadron

In accordance with AFI 33-219, I have determined that the notification actions outlined in your summary letter are sufficient to provide reasonable notice to all personnel using DOD telecommunications systems that such use constitutes consent to telecommunications monitoring.

L. LAWYER, Col, USAF

Judge Advocate

Attachment 5

IC 2006-1 TO AFI 33-219, TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM (TMAP)

1 MAY 2006

OPR: HQ AIA/DO (Col Ronald Haygood)

Certified by: SAF/XCIA (Col Gary W. Klabunde)

Supersedes AFI 33-219, 23 May 2002

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will become *Information Assurance*), and prescribes responsibilities, procedures, and guidance concerning the Telecommunications Monitoring and Assessment Program (TMAP). It also implements national and Department of Defense (DOD) directives pertaining to the monitoring of unsecured telecommunications for information content and establishes a requirement for feedback in the operations security (OPSEC) process AFPD 10-11, *Operations Security* (will be superseded by AFPD 10-7, *Information Operations*). Guidance in Air Force Instruction (AFI) 71-101, Volume 2, *Protective Service Matters*, concerning telephone interception and eavesdropping does not apply to telecommunications monitoring conducted according to this instruction. AFPD 10-20, *Air Force Defensive Counterinformation Operations* (will be superseded by AFPD 10-7), requires OPSEC participation as part of its employment capabilities for Defensive Counterinformation (DCI) operations to protect and defend DOD/Air Force information and information systems. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by the DOD that operate information systems. Certain aspects of this instruction apply to all users of Air Force-controlled DOD telecommunications systems, equipment, and devices. This instruction applies to the Air National Guard (ANG). Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, provides more current background for OPSEC relationships. Find additional security instructions and manuals on the Air Force Publishing Web Site at <http://www.e-publishing.af.mil> under Electronic Publications. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. **Failure to observe the prohibitions and mandatory provisions of this instruction in paragraphs 21.8. and 21.9. by military personnel is a violation of Article 92, Uniform Code of Military Justice. Violations by civilian employees may result in administrative or disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.** Direct questions or comments on the content of this instruction to Headquarters Air Intelligence Agency (HQ AIA/DO), 102 Hall Blvd, Suite 115A, San Antonio TX 78243-7029. Refer suggested changes or conflicts between this and other instructions through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/EASD), 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, using Air Force (AF) IMT 847, **Recommendation for Change of Publication.** Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363) and disposed of in accordance with Air Force Records Information Management System (AFRIMS), *Records Disposition Schedule (RDS)* located at https://afrims.amc.af.mil/rds_series.cfm. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This change incorporates interim change IC 2006-1 (Attachment 5). It updates organization names, office symbols and references. This change adds responsibilities for the commanders of Air Combat Command

(ACC) (paragraph 7.1), Eighth Air Force (paragraph 7.2) and the 67th Information Operations Wing (paragraph 7.3). It properly aligns oversight and focal point responsibility for monitoring telecommunications systems to HQ USAF/A3I (paragraph 7). This change clarifies the notice and consent requirement for private/intranet unit homepages (paragraph 13.8.3 and A3.3.6.3). It updates the title of Section D, clarifies the annual TMAP assessment requirements in paragraphs 17 and the tasking priorities in 17.2, adds tasking priorities for HQ AIA/DO (paragraph 17.3) and removes guidance on out-of-cycle TMAP requests (paragraph 19). This change identifies the proper coordination channels on the use of TMAP information for law enforcement and adverse actions (paragraph 25). Paragraph 27.2 was updated to reflect the AFRIMS website. Additionally, the mandatory notice and consent procedures in Attachment 3 were clarified to include the requirements for Personal Electronic Devices (paragraph A3.3.4), expanded examples of computer systems (paragraph A3.3.6), expanded guidance for computer system log-on banners (paragraph A3.3.6.1), requirements for systems with financial or technical limitations to the log-on banner installation (paragraph A3.3.6.2), and requirements for private/intranet unit homepages (paragraph A3.3.6.3). The example in Attachment 4 was updated to reflect the clarified guidance in Attachment 3. A bar (|) indicates a revision from the previous edition.

5. The Assistant Secretary of Defense/Networks and Information Integration (ASD/NII). 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 provides 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. The requesting unit provides information copies to Headquarters United States Air Force (HQ USAF/A3I), 1630 Air Force Pentagon, Room 4E1046, Washington DC 20330-1630. HQ AIA/DO reviews the request as soon as possible, and if capable of supporting the request, pursues the ASD/NII approval.

7. HQ USAF/A3I. Provides oversight, advocacy and acts as the focal point for TMAP according to AFI 10-701, *Operations Security*.

7.1. Commander, Air Combat Command (ACC):

7.1.1. Provide TMAP operations in support of OPSEC assessment capabilities for the Air Force.

7.1.2. Coordinate with the Joint Staff, the National Security Agency, or other DoD components for monitoring telecommunications systems that carry both Air Force and other government agency information.

7.2. Commander, Eighth Air Force (8 AF/CC). Designated by the Chief of Staff of the Air Force as the overall tasking authority for TMAP operations to be conducted at any time on any Air Force installation certified by SAF/GC as compliant with established notice and consent procedures.

7.3. Commander, 67th Information Operations Wing (67 IOW). Delegated by the 8 AF/CC to be the operational tasking authority (see paragraph 17) for TMAP operations to be conducted at any time on any Air Force installation certified by SAF/GC as compliant with established notice and consent procedures.

8. Secretary of the Air Force, Information, Services and Integration Directorate, Information Assurance Division (SAF/XCIA). This is the lead office within the Air Force for policy matters affecting notice and consent certification and related issues.

9. Headquarters Air Force Communications Agency (HQ AFCA).

9.1. HQ AFCA/EVP notifies the MAJCOM, FOA, and DRU Information Assurance (IA) offices in early February during even-numbered fiscal years to initiate biennial notification procedures.

9.2. HQ AFCA/EVP acts as the focal point for the notice and consent certification process.

11.6. Maintain documentation (Attachments 1 through 6 of example) in Attachment 4 of this AFI, at MAJCOM, FOA, and DRU-level.

13.7.2. Ensure compliance with notice and consent requirements by annually checking Wing information systems subject to monitoring according to AFI 33-230, *Information Assurance Assessment and Assistance Program*.

13.8.3. Ensure the **first pages** on all the unit's private/intranet web homepages comply with **Attachment 3**. (NOTE: Notice and consent requirements do not apply to public web sites/pages. See AFI 33-129, *Web Management and Internet Use*, for Privacy and Security Notice requirements for public web sites/pages.)

16.3. MAJCOM, FOA, and DRU IA Offices. These offices ensure all subordinate bases and installations under their control respond in a timely manner and that the information provided in the package complies with the requirements of this instruction. The MAJCOM, FOA, and DRU IA offices send the completed summary report and documentation to the MAJCOM, FOA, and DRU SJA for review. Following this legal review (and correction of any deficiencies noted), the MAJCOM, FOA, and DRU IA offices sends the summary report and SJA determination to HQ AFCA/EVP, 203 W. Losey, Room 2200, Scott AFB IL 62225-5222. Submit these reports by 15 May of each even-numbered year.

16.4. HQ AFCA/EVP. This office ensures all USAF facilities submit inputs in order to receive biennial SAF/GC certification. This office sends all summaries and SJA determinations to HQ AFCA/JA for review and endorsement. TMAP files containing insufficient evidence of monitoring notice and consent as required by this instruction are returned to the appropriate MAJCOM IA offices for follow-on corrective action. HQ AFCA/EVP sends all summaries of actions to SAF/GC, 1740 Air Force Pentagon, Room 4E856, Washington, DC 20330-1740, by 15 July each even-numbered fiscal year.

16.5. SAF/GC. Certifies sufficient notice of TMAP monitoring is provided to users of DOD telecommunications systems of specific USAF installations and authorizes use of TMAP assessments at approved installations. If the General Counsel determines the base summary report contains insufficient evidence to establish full compliance with notice of monitoring requirements, the summary is returned for further corrective action prior to certification. This office returns a certification listing to HQ AFCA/EVP by 1 September of each even-numbered fiscal year, listing installations approved to receive TMAP assessments. This certification listing is valid for 2 years expiring on 30 September.

Table 1. TMAP Certification Schedule.

Even Year Date	Office	Action
Early Feb	HQ AFCA/EVP	Initiates Biennial notification procedures
15 Feb – 15 Apr	Wing IA Office	Prepares Summary
15 Apr	Wing IA Office	Sends Summary to Base SJA
1 May	MAJCOM, FOA, and DRU IA Office	Reviews Summary and MAJCOM, FOA, and DRU SJA Review
15 May	MAJCOM, FOA, and DRU IA Office	Sends Summary to HQ AFCA/EVP with MAJCOM, FOA, and DRU SJA endorsement
15 May - 15 Jul	HQ AFCA/EVP	Reviews all Summaries with HQ AFCA/JA
15 Jul	HQ AFCA/EVP	Sends summaries to SAF/GC
1 Sep	SAF/GC	Provides HQ AFCA/EVP with a list of bases approved to continue TMAP monitoring
15 Sep	HQ AFCA/EVP	Releases a message listing certified bases

Section D - Obtaining Telecommunications Monitoring Assessments

17. Identifying Monitoring Requirements. Air Force organizations desiring TMAP/Electronic System Security Assessments (ESSA) support identify their requirements to the 67 IOW's ESSA Tasking Cell (ETC), 67th Operations Support Squadron (OSS), for scheduling and prioritization. Each January, HQ AIA/DO requests all MAJCOMs, FOAs and DRUs provide TMAP assessment requirements based on HQ AIA/67 IOW ESSA program enhancements for the proceeding fiscal year. MAJCOMs, FOAs, and DRUs respond by 15 July of each year with TMAP assessment requests. By 15 September, the 67 IOW tasks HQ AIA TMAP elements based on requests submitted. For customers with an established continuous monitoring tasking, review the tasking document annually by 1 October and update as warranted with current signatories. This tasking document constitutes authority for TMAP elements to operate, if the installations scheduled for monitoring are currently certified by SAF/GC.

17.2.1. Priority 1. Contingency operations.

17.2.1.1. 1A. Combat planning cells.

17.2.1.2. 1B. Combat enabling forces.

17.2.1.3. 1C. Military Operations Other than War.

17.2.2. Priority 2. Special Access Programs (SAP) and research, development, test and evaluation (RDT&E) of USAF Emerging Technologies.

17.2.2.1. 2A. Existing SAPs.

17.2.2.2. 2B. Test and Evaluations.

17.2.2.3. 2C. Research and Development.

17.2.3. Priority 3. Air Expeditionary Force predeployment exercises/events.

17.2.4. Priority 4. Joint Chiefs of Staff directed exercise.

17.2.5. Priority 5. Combatant command/MAJCOM exercises.

17.2.6. Priority 6. Baseline assessments.

17.2.7. Priority 7. All other requirements.

17.3. Biannual Requirements and Tasking Priorities. Each September and April, HQ AIA/DO requests Community of Interest (COI) members identify TMAP requirements for scheduled Air Force events/operations (exercises, reoccurring events, baseline OPSEC assessments, etc). The ETC consolidates and prioritizes all scheduled and ad-hoc requirements identified by the COI in accordance with the tasking priority list. The ETC then tasks worldwide TMAP units using an ESSA Tasking Order.

18.2. If JCMA is not designated as the Executive Agent for telecommunications monitoring, unified or specified commands coordinate with the ESSA Tasking Cell, through the Air Force component command as a member of the COI. Execute requirements in accordance with AFMAN 10-401.

19. DELETED

25. Using Telecommunications Monitoring and Assessment Program (TMAP) Information for Law Enforcement and Adverse Actions. Information acquired during the course of an authorized TMAP operation that is provided to Air Force officials pursuant to paragraph 24.5, may not be used for adverse administrative or disciplinary actions against an individual identified through such TMAP information without submitting the matter through HQ AIA/DO/JA to HQ USAF/A3II and SAF/GC. Information obtained during TMAP operations may not be used for adverse administrative or disciplinary actions without the approval of SAF/GC.

27.2. Records: Maintain and dispose of records created by this publication in accordance with AFRIMS RDS, Table 33-24, Rule 1, 5, 7, 8, and 9, is located at https://afrims.amc.af.mil/rds_series.cfm.

MICHAEL W. PETERSON, Lt Gen, USAF

Chief of Warfighting Integration and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSM 3122.03A, *Joint Operations Planning and Execution System, Volume II, Planning Formats and Guidance*, 31 December 1999, C1, 6 September 2000

Paperwork Reduction Act of 1995

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

DODD 4640.6, *Communications Security Telephone Monitoring and Recording*, 26 June 1981 (Note: to be superseded by DODD 8560.aa)

DODM 4525.8-M, AF Sup 1, *Official Mail Manual*

AFDD 2-5, *Information Operations*

AFPD 10-11, *Operations Security* (will be superseded by AFPD 10-7, *Information Operations*)

AFPD 10-20, *Air Force Defensive Counterinformation Operations* (will be superseded by AFPD 10-7, *Information Operations*)

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

AFI 10-701, *Operations Security*

AFI 33-129, *Web Management and Internet Use*

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

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*

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

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

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

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

Abbreviations and Acronyms

8th AF—Eighth Air Force

67 IOW—67th Information Operations Wing

67 OSS—67th Operations Support Squadron

AF—Air Force (when used on forms)

AFCA—Air Force Communications Agency

AFDD—Air Force doctrine document

AFDIR—Air Force Directory

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force policy directive

AFRIMS—Air Force Records Information Management System

AIA—Air Intelligence Agency

ANG—Air National Guard

ASD—Assistant Secretary of Defense

CI—critical information

CJCSM—Chairman of the Joint Chiefs of Staff manual
COI—community of interest
COMSEC—communications security
DCI—Defensive Counterinformation Operations
DOD—Department of Defense
DRU—direct reporting unit
DTS-W—Defense Telecommunications Service-Washington
DV—distinguished visitor
E-mail—electronic mail
ESSA—electronic system security assessment
ESSAC—Electronic System Security Assessment Central
ETC—ESSA tasking cell
FOA—field operating agency
IO—Information operations
IA—Information assurance
JCMA—Joint COMSEC Monitoring Activity
JCS—Joint Chiefs of Staff
LMR—land mobile radio
MAJCOM—major command
MDVA—multiple discipline vulnerability assessment
NCR—National Capital Region
NII—network and information integrity
OPFOR—opposition forces
OPR—office of primary responsibility
OPSEC—operations security
PED—portable electronic device
POC—point of contact
PPI—personal privacy information
RCS—Reports Control Symbol
RDS—Records Disposition Schedule
RDTE—Research, Development, Test and Evaluation
SAF—Secretary of the Air Force

SAP—Special Access Program

SJA—Staff Judge Advocate

TAR—Telecommunications Assessment Report

TMAP—Telecommunications Monitoring and Assessment Program

TPFDD—Time Phased Force Deployment Document

U.S.—United States

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 Content—When used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. It does not include communication routing information including Internet Protocol addresses or machine-readable binary packets in a packet switched network used to direct or route the communication.

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

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.

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, FOA, and DRU 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.

Unprotected Telecommunications—Telecommunications that do not use authorized unclassified Public Key Encryption products.

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 that does not use authorized cryptographic products or protected distribution systems.

Attachment 3

NOTICE AND CONSENT PROCEDURES

A3.1. Educate personnel about the hostile signal intelligence threat to unsecured telecommunications.

A3.2. Provide guidance to users in the proper use of unsecured telecommunications.

A3.3. Notify users of DOD telecommunications devices, including contractors and their employees, that using DOD telecommunications systems constitutes consent to telecommunications monitoring. The following notification procedures are **mandatory** for official DOD telecommunications systems/devices:

A3.3.1. Installation telephone directories. Prominently display the following notice and consent statement on the front cover of telephone directories, or, if the telephone directory is embedded in a base information guide this notice must precede the telephone directory portion of the base guide: **“DO NOT DISCUSS CLASSIFIED INFORMATION ON UNSECURE TELEPHONES. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES.”** **“DOD telephones are provided for the transmission of official government information only and are subject to communications security monitoring at all times. Use of official DOD telephones constitutes consent to communications security telephone monitoring in accordance with DOD Directive 4640.6.”** This banner is also required on the top of the first page of the electronic version of the telephone directory.

A3.3.2. Telephones.

A3.3.2.1. Affix DD Form 2056, **Telephone Monitoring Notification Decal**, on the front of all official telephones.

A3.3.2.2. For telephones with secure voice capability that can be used in the unsecure mode, such as Secure Telephone Unit, Secure Terminal Equipment, etc., remove the words **“DO NOT DISCUSS CLASSIFIED INFORMATION”** from the form.

A3.3.3. Facsimile Machines. Both of the following actions are required to notify users of facsimile machines:

A3.3.3.1. DODM 4525.8-M, AF Sup 1, *Official Mail Manual*, mandates the use of AF IMT 3535, **Facsimile Electro Mail Transmittal**, when a cover sheet is required for fax transmission. The AF IMT 3535 contains the proper notice and consent statement. If any other cover sheet is used, the following notice and consent statement must be printed on it: **“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.”**

A3.3.3.2. Affix the DD Form 2056, on all facsimile machines.

A3.3.4. Portable Electronic Devices (PED) (e.g., text pagers, personal digital assistants, and cellular telephones) must meet one or both of the following requirements.

A3.3.4.1. When issued the device, require personnel to sign a form that includes the following notice and consent statement: **“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.”** The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.3.4.2. Affix the DD Form 2056 on all PEDs.

A3.3.5. Hand-held radios/land mobile radios (LMR) must meet one or both of the following requirements.

A3.3.5.1. Affix the DD Form 2056 on all hand-held radios/LMRs or:

A3.3.5.2. Sign a form that includes the statement in A3.3.4.1. The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.3.6. Put users of official computer systems (includes but is not limited to computers connected to a network, servers, stand-alone computers, portable computers, routers) and private/intranet web pages on notice their use constitutes consent to monitoring as specified in the notice and consent log-on banner cited below.

“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.”

A3.3.6.1. Install the notice and consent log-on banner on all computers. The banner is automatically displayed upon boot-up and/or initial log-on for the computer system regardless of the access methodology (physical, network, remote access, dial-in, etc.). Place the banner on the computers in such a way that the user must press a key to get beyond it, thereby demonstrating acceptance of its provisions.

A3.3.6.2. For systems where it is not cost effective or technically feasible to install the complete notice and consent log-on banner cited above, as determined by the MAJCOM/A6, perform at least two of the following requirements:

A3.3.6.2.1. Affix the notice and consent warning banner (DD Form 2056) on all computer monitors or video display screens of those systems.

A3.3.6.2.2. Users of the system (regardless of access methodology) must sign a receipt statement including the following statement: **This is a Department of Defense system. This system is for authorized U.S. Government use only. This system is subject to monitoring at all times. Using this system constitutes consent to monitoring.** The signed forms will be retained by the office managing the system until 6 months after the user no longer requires access to the system.

A3.3.6.2.3. Install the following, abbreviated log-on banner on the system: **“This is a Department of Defense system. This system is for authorized U.S. Government use only. This system is subject to**

monitoring at all times. Using this system constitutes consent to monitoring.” Use of this option may be appropriate for systems with technical limitations on the amount of text used for initial login notices.

A3.3.6.3. Private/intranet Web Homepages. Prominently display the notice and consent banner on the first pages of ALL the unit's private/intranet web homepages.

A3.3.7. Any telecommunications devices not otherwise referenced in this attachment must have a DD Form 2056 affixed or the person to whom the device is issued must sign a receipt statement including the following statement: **“This telecommunications device is subject to monitoring at all times. Using this device constitutes consent to monitoring.”** The signed forms will be retained by the office issuing the device until 6 months after the device is returned.

A3.4. Optional methods to get this information to Air Force personnel are:

A3.4.1. Correspondence from the base or facility commander, addressing proper use of unsecured telecommunications, to all assigned units for dissemination to unit personnel.

A3.4.2. Addressing telecommunications issues to newcomers during in-processing, periodic OPSEC awareness briefings, and commander's calls.

A3.4.3. Using base bulletins, base newspapers, E-mails, web pages, and similar publications on a periodic basis.

A3.4.4. Incorporating notice and consent comments in operating procedures, instructions, etc., that are periodically reviewed by users.

A3.4.5. 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 4**EXAMPLE OF NOTICE AND CONSENT MEMORANDUM AND 1ST IND**

MEMORANDUM FOR: Supporting Legal Office

FROM: XX COMMUNICATIONS SQUADRON

Anywhere AFB 12345

SUBJECT: Summary of Consent Notification Actions Taken During the Two-Year Period From 1 Apr XX - 31 Mar XX (RCS: HAF-SC(BE)9497)

The following actions were taken during the past 2 years to notify users of DOD telecommunications devices that using the telecommunications devices constitutes consent to telecommunications monitoring for Anywhere AFB (and the following Geographically Separated Units: [list]).

a. The current base telephone directory, dated _____, includes the notice and consent statement on the front cover, or on first page of the official portion of the phone book, in accordance with AFI 33-219 (version date), paragraph A3.3.1 (see Attachment 1). An electronic version of the telephone directory is available on the base Intranet and the notice and consent statement is on the top of the first page (see Attachment 2). **NOTE:** If your base does not have a hard copy phone directory or an electronic phone directory state so in this paragraph.

b. All telephones were inspected on (date) and ___% of all phones had the DD Form 2056 attached. Decals were immediately applied to all non-compliant telephones. Consequently, all telephones have DD Form 2056 affixed as of the date of this report.

c. All faxes were inspected on (date) and ___% of all machines have the DD Form 2056 affixed. Decals were immediately applied to all non-compliant fax machines. Consequently, all faxes have DD Form 2056 affixed as of the date of this report. Use either AF IMT 3535 or another cover sheet that includes the statement in AFI 33-219 (version date), paragraph A3.3.3.1. A sample of a fax cover sheet is attached (see Attachment 3). **NOTE:** Do not submit a copy of AF IMT 3535.

d. On (date) it was verified that all individuals issued an official portable electronic device (including but not limited to cell phone, text pager, and personal digital assistants) had the DD Form 2056 affixed to the device and/or signed a receipt that includes the notice and consent statement contained in AFI 33-219 (version date), paragraph A3.3.4.1 (see Attachment 4).

e. All LMRs were inspected on (date) and ___% of all instruments had the DD Form 2056 affixed, or it was verified that all individuals issued an LMR/hand-held radio have signed a receipt that includes the notice and consent statement contained in AFI 33-219 (version date), paragraph A3.3.4.1 (see Attachment 4). Decals were immediately affixed to all non-compliant LMRs. Consequently all LMRs have DD Form 2056 affixed or all users have signed the required receipt notice. A sample of letter/receipt for all devices is attached.

f. The notice and consent banner, in accordance with AFI 33-219 (version date), paragraph A3.3.6., has been installed on all computer systems (including but not limited to computers connected to a network, servers, stand-alone computers, portable computers and routers). The banner is automatically displayed upon boot-up and/or initial log-on for the computer system regardless of the method accessed (see Attachment 5). All computers were inspected and ___% of all computers displayed the log-on banner. The banner was immediately installed on all non-compliant computers. Consequently, all computers display the log-on as of the date of this report.

g. The current notice and consent banner is prominently displayed on the first pages of ALL of the unit's private/intranet web homepages. The warning banner is worded exactly as the log-on banner shown in AFI 33-219 (version date), paragraph A3.3.6. A print screen copy of the web page is attached (see Attachment 6).

h. TMAP training was provided to all unit/squadron personnel. This training requirement will be part of the initial and recurring OPSEC training.

i. Other notification actions: (List any optional methods (AFI 33-219, paragraph A3.4) used to notify unit/squadron personnel.)

JOE DOE, Lt Col, USAF
Commander

6 Attachments

1. Telephone Directory Cover**
2. Print Screen of Electronic Telephone Directory Web Page**
3. Copy locally produced FAX cover sheet, if used**(must have the notice and consent statement on it)
4. Portable Electronic Device Notification Form/LMR**
5. Print Screen of Computer Banner**
6. Print Screen of Unit Private Web Pages with Banner**

**Mandatory attachment

1st Ind, JA 12 Apr 00

TO: 123d Communications Squadron

In accordance with AFI 33-219, I have determined that the notification actions outlined in your summary letter are sufficient to provide reasonable notice to all personnel using DOD telecommunications systems that such use constitutes consent to telecommunications monitoring.

L. LAWYER, Col, USAF
Judge Advocate