BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-712

8 JUNE 2011

Incorporating Change 1, 8 March 2012

Operations

TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM (TMAP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A3Z-CI

Certified by: AF/A3Z (Maj Gen Bolton)

Supersedes: AFI 33-219, 1 May 2006

Pages: 45

This Instruction implements Air Force Policy Directive (AFPD) 10-7, *Information Operations*. It also, implements the guidance in Department of Defense Instruction (DoDI) 8560.01, *Communications Security (COMSEC) monitoring and Information Assurance (IA) Readiness Testing* and is consistent with the policy established in AFPD 33-2, *Information Assurance*. It prescribes responsibilities, procedures, and guidance for the Telecommunications Monitoring and Assessment Program (TMAP). It also conforms to national and Department of Defense (DoD) directives pertaining to the monitoring of unsecured telecommunications for information content. This publication applies to all military, civilian and contractor personnel under contract to the DoD, who use Air Force controlled DoD telecommunications systems, equipment, and devices and to those who operate, connect, or interact with information systems owned, maintained, and controlled by the DoD. This includes all information technology used to process, store, display, transmit, or protect DoD information, regardless of classification or sensitivity. It applies to members, employees, and contractors in Air Force Reserve (AFR) and to the Air National Guard (ANG). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. All reporting requirements in this AFI are exempt from licensing IAW AFI 33-324, *The Information Collections and Reports Management Program, Controlling Internal, Public and Interagency Air Force Information Collections,* paragraph 2.11.1. **Failure to observe the prohibitions and**

mandatory provisions of this Instruction in paragraphs 3.2, and all of its subparagraphs by military personnel is a violation of Article 92, *Uniform Code of Military Justice*. Violations by civilian or contract employees may result in administrative or disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

SUMMARY OF CHANGES

This interim change implements new guidelines that clarify requirements for the telecommunications monitoring assessment program (TMAP). An asterisk indicates newly revised material.

Chapter 1—GENERAL **4**

1.1. Introduction. 4

1.2. Purpose. 4

1.3. Notice and Consent (N&C). 5

1.4. Roles, and Responsibilities. 6

Chapter 2—TMAP PRODUCTS **15**

2.1. There are two basic types of TMAP products 15

2.2. Products. 15

2.3. Reports. 15

2.4. Transcripts. 16

2.5. Combining Products. 16

Chapter 3—TMAP PROCEDURES **17**

3.1. Assessment Request Procedures and Process Flow (See Figure 3. 17

Figure 3.1. TMAP Request Process Flow 18

3.2. Use and Control of Products; Situational Guidance. 18

3.3. Transcript Release Procedures. 21

Figure 3.2. Unsanitized Transcript Process 22

3.4. Team Support. 22

Chapter 4—NOTICE AND CONSENT PROCEDURES **24**

4.1. Notification. 24

4.2. Telephone Directories. 24

4.3. Telephones. 24

4.4. Facsimile Machines. 24

4.5. Information Systems. 24
4.6. Private or Intranet Web Homepages. 25
4.7. Portable Electronic Devices (PED). 25
4.8. Other Information Technology. 26
4.9. Optional Notice and Consent Awareness Methods. 26
4.10. Certification Process. 26
4.11. Notice and Consent Certification Schedule. 29
Table 4.1. Notice and Consent Certification Schedule 29

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 31

Attachment 2—SAMPLE TMAP REPORTS 35

Attachment 3—STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER 37

Attachment 4—MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS 38

Attachment 5—(Template) NOTICE AND CONSENT MEMORANDUM WITH 1ST AND 2ND IND 40

Attachment 6—NOTICE AND CONSENT CHECKLIST 43

Chapter 1

GENERAL

1.1. Introduction. The Air Force (AF) uses telecommunications systems such as telephones, cellular phones, radios, facsimile, pagers, computer networks, internet-based capabilities (IbC) such as blogs, web-sites, social networking sites, etc., and other wired or wireless electronic devices to conduct day-to-day official business. Adversaries can easily monitor these systems to gather information regarding military capabilities, limitations, intentions, and activities. The Telecommunications Monitoring and Assessment Program (TMAP) provides commanders with an assessment as to the type and amount of information traversing telecommunications systems at risk to adversary collection and exploitation. TMAP products should be used to evaluate personnel compliance with Information Protection (IP) practices and coordination of Military Deception or Signature Management activities. TMAP products are also used to support other security programs/activities, enhance force protection, and focus training requirements. **Note:** For the purposes of this AFI, the terms telecommunications systems, communications systems, and information systems will be synonymous. The terms telecommunications and communications will also be synonymous.

1.2. Purpose. The Air Force conducts communications monitoring, through TMAP, to support Operations Security (OPSEC) for each of the AF Core Functions: Nuclear Deterrence Operations, Air Superiority, Space Superiority, Cyberspace Superiority, Global Precision Attack, Rapid Global Mobility, Special Operations, Global Integrated Intelligence, Surveillance and Reconnaissance, Command and Control, Personnel Recovery, Building Partnerships and Agile Combat Support. TMAP involves the collection and analysis of information transmitted via unsecured telecommunications systems. These systems can include radios and wired or wireless telephones, facsimiles, or computer networks. The assessment function of this program can help determine if these systems are transmitting critical, sensitive, or classified information. TMAP products help evaluate an organization's IP posture and determine the amount and type of information available to adversary collection entities. TMAP is only accomplished by designated units and within certain legal parameters.

1.2.1. The AF monitors official unsecured and unprotected telecommunications systems to determine if they are being used to transmit critical, 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 US (and allied/coalition) operations. Information can be provided near real-time as a force protection tool or systematically collected, analyzed, data based, and reported to major command (MAJCOM), direct reporting units (DRU) and field operating agencies (FOA), as long-term information liabilities.

1.2.2. The AF conducts two types of TMAP assessments no-notice and organization requested. A no-notice assessment is conducted at the direction of 24 AF/CC without having to receive concurrence or provide prior notification to the organization. Organization requested assessments are submitted by the AF, MAJCOM, DRU, or FOA OPSEC Program Manager (PM) to the 624th Operating Center (OC). All TMAP assessments are at no cost to the assessed organization. Refer to paragraph 3.1 for further details. Monitoring resources

may be 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. These assessments are also conducted to provide information and data into the information operations risk analysis process; gauge the overall effectiveness of a program or operation; and to support information assurance (IA) objectives.

1.2.3. TMAP is an integral part of the AF OPSEC and Information Operations (IO) Red Teaming, and defense critical infrastructure (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 provides known threat information.

1.2.4. TMAP is not an Intelligence mission and organizations conducting TMAP are not required to comply with Intelligence Oversight directives with respect to those activities.

1.2.5. TMAP mission subsets available to a commander include:

1.2.5.1. Telephony Communications – assessment of AF unclassified voice networks which if exploited by adversaries, can negatively impact AF operations.

1.2.5.2. Radio Frequency (RF) Communications - assessment of AF communications within the VHF, UHF, FM, HF, and SHF frequency bands (mobile phones, LMRs, wireless LANs) which if exploited by adversaries, can negatively impact AF operations.

1.2.5.3. E-mail Communications – assessment of unclassified AF email traffic traversing the AFNet which if exploited by adversaries, can negatively impact AF operations.

1.2.5.4. Internet based Capabilities (IbC) - assessment of information posted to all publicly accessible information capabilities and applications available across the internet in locations not owned, operated, or controlled by the Department of Defense (DoD) or the Federal Government, which originate within the AFNet. **NOTE:** TMAP units are only monitoring the information leaving the AFNet and not the IbC sites themselves. IbCs include collaborative tools such as social networking sites (SNS), social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps, etc.)

1.2.5.5. Web Risk Assessment (WRA) – assessment of information posted on AF unclassified owned, leased, or operated public and private web sites in order to minimize exploitation of AF information by adversaries that can negatively impact AF operations.

1.2.5.6. Cyber Operations Risk Assessment (CORA) – an assessment of data compromised through intrusions of AF networks with the objective of determining the associated impact to operations resulting from that data loss to adversaries.

1.3. Notice and Consent (N&C). All authorized users of telecommunications systems and devices must receive legally sufficient notice that monitoring is conducted and that use of the system or device constitutes consent to monitoring. All DoD telecommunications systems and information systems are subject to monitoring for authorized purposes as prescribed by DoDI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA)*

Readiness Testing, DoDD 5205.02, *Operations Security (OPSEC) Program,* and AFI 33-200, *Information Assurance (IA) Management*.

1.3.1. **Objectives.** Compliance with legal requirements associated with notifying personnel of telecommunications monitoring and their consent by using these devices.

1.3.1.1. Ensure notice and consent actions are implemented in a legally sufficient manner to permit initiation or continuation of monitoring activities at all Air Force installations and on all Air Force telecommunication and information systems according to DoDI 8560.01.

1.3.1.2. Provide implementation guidance for the exact content of a warning banner as specified by current DoD direction (see Attachment 3 and 4 for reference).

1.3.1.3. Establish a primary reference and additional implementation guidelines for IA Control ECWM-1, Warning Message, according to the requirements of DoDI 8500.02, *Information Assurance Implementation*.

1.3.1.4. Establish guidance and provide procedures for accomplishment of the biennial IA notice and consent certification according to DoDI 8560.01.

1.3.1.5. For complete details on the procedures for N&C certification (see Chapter 4).

1.4. Roles, and Responsibilities.

1.4.1. **Joint Communications Security (COMSEC) Monitoring Activity (JCMA)**. JCMA conducts communications monitoring across the DoD. JCMA may request Air Force support for its tasked missions through HQ USAF. JCMA requests should be levied as a joint requirement and executed under the Joint Operations Planning and Execution System.

1.4.2. **Assistant Secretary of Defense/Networks and Information Integration (ASD/NII)** 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 communications services to DoD elements located in the National Capitol Region.

1.4.3. **Secretary of the Air Force (SECAF)** per DoDI 8560.01 approves COMSEC monitoring and IA readiness testing of AF owned or leased systems. This authority may be delegated.

1.4.4. **The Secretary of the Air Force General Counsel (SAF/GC)** provides oversight and guidance on all matters pertaining to TMAP procedures and activities. Reviews and approves all adverse or disciplinary personnel actions when based on TMAP information. Also certifies that Air Force installations meet legal requirements to allow communications monitoring.

1.4.4.1. Authorizes initiation or continuation of IA and OPSEC monitoring at installations that provide legally adequate notice to users of DoD telecommunications systems, equipment, and devices that such use constitutes consent to monitoring.

1.4.4.2. Biennially, during even-numbered fiscal years, reviews reports prepared in accordance with Attachment 5, forwarded by each AF installation, certifying accomplishment of mandatory notice and consent actions over the previous 24 months.

1.4.5. **Administrative Assistant to the Secretary of the Air Force (SAF/AA)** provides coordination and integration of TMAP policy and guidance through the Air Force Security Policy Oversight Board (AFSPOB).

1.4.6. **Secretary of the Air Force, Office of Public Affairs (SAF/PA)** develops policy and guidance on the process for releasing information to the public.

1.4.6.1. Ensure public Web sites receive initial security and policy review prior to site launch. PA must assess the need, requirement, and suitability for release of information.

1.4.7. **Secretary of the Air Force Office of Information Dominance and Chief Information Officer (SAF/CIO A6):**

1.4.7.1. Proposes policy for matters affecting notice and consent certification and related matters.

1.4.7.2. Ensure a current AF White List is provided to TMAP PMO so they can identify approved registered AF owed, operated, and leased web sites.

1.4.7.3. Ensure those performing IA readiness testing receive formal training; are fully competent in using the tools, techniques, and procedures associated with such activities; and properly understand their duties and the relevant legal requirements.

1.4.8. **Deputy Chief of Staff for Operations, Plans, and Requirements (AF/A3/5).** The Director of Operations; Directorate of Cyber and Space Operations (AF/A3Z) is the OPR for establishing TMAP policy and guidance. AF/A3Z will:

1.4.8.1. Provide oversight, advocacy, and act as a focal point for TMAP.

1.4.8.2. Develop Air Force Departmental publications to define policy, guidance, responsibilities, and authorities to establish the internal management processes necessary to carry out DoD policy/guidance.

1.4.8.3. Ensure those performing TMAP monitoring receive formal training; are fully competent in using the tools, techniques, and procedures associated with such activities; and properly understand their duties and the relevant legal requirements.

1.4.8.4. Facilitate the establishment of a Program Management Office (PMO) under the authority and direction of HQ Air Force Space Command.

1.4.8.5. Advocate for program funding for TMAP through established budgeting and requirements process.

1.4.8.6. Coordinate assessment procedures with joint staff, National Security Agency, and other DoD components when joint systems carry AF communications of interest.

1.4.9. **Air Force Space Command, Directorate of Air, Space, and Cyber Operations (AFSPC/A3).** The TMAP mission falls under AFSPC/A3I, Cyber Operations Capability and the TMAP Program Management Office (PMO) will:

1.4.9.1. Organize, train, and equip forces to provide combatant commanders with TMAP capabilities.

1.4.9.2. Fulfill Air Force requirements for communications monitoring.

1.4.9.3. Provide TMAP resources to assist other AF organizations to assess their telecommunications.

1.4.9.4. Ensure TMAP focuses on the collection and analysis of information transmitted via unsecured communications systems.

1.4.9.5. Develop funding documents to procure improved capabilities and ensure maintenance of these capabilities.

1.4.9.6. Comply with appropriate AF acquisition, evaluation, and contracting processes.

1.4.9.7. Coordinate assessment capabilities with the Joint Staff, NSA, and other DoD Components to standardize equipment/processes and increase interoperability.

1.4.9.8. Generate new ideas and concepts to continuously improve TMAP.

1.4.9.9. Conduct vulnerability assessments of information that transverses the AF Global Information Grid and is placed on IbC platforms.

1.4.9.10. Integrate TMAP Cyber Operations Risk Assessment (CORA) capabilities into the overall AF Information Damage Assessment process.

1.4.9.11. Develop operational capability requirement documents for conducting TMAP.

1.4.9.12. Establish and maintain at the MAJCOM level a TMAP PMO.

1.4.9.13. Deleted

1.4.9.14. Deleted

1.4.9.15. Deleted

1.4.9.16. Deleted

1.4.9.17. Consider the integration and use of TMAP and/or TMAP products with other Information Protection/security support capabilities, efforts or initiatives.

1.4.9.18. Authorize telecommunications monitoring procedures.

1.4.9.19. Deleted

1.4.9.20. Deleted

1.4.9.21. Provide quarterly reports to AF/A3Z-CI, by the 15th day of the following quarter (15 Jan, 15 Apr, 15 Jul, 15 Oct) regarding the assessment of potential critical information found during TMAP operations. Such as information derived from emails, telephone conversations, LMRs, AF Social Media Sites, AF Blogs, AF Public and Private Web Sites, and/or data which was exfiltrated from AF networks via CORA.

1.4.10. **Air Force Space Command, Directorate of Communications and Information and AFSPC Chief Information Officer (AFSPC/A6).** The N&C mission falls under AFSPC/A6. AFSPC/A6 will:

1.4.10.1. Review, and evaluate national and DoD notice and consent guidance, and makes recommendations on implementation to SAF/CIO A6.

1.4.10.2. Biennially, during even numbered fiscal years:

1.4.10.2.1. Coordinates with MAJCOM, DRU, FOA, and Wing IA offices to prepare for biennial reporting procedures.

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

1.4.10.2.3. Develops, and coordinates, notice and consent policy and guidance with AF/A3Z.

1.4.10.2.4. Maintain copies of installation Notice & Consent Memorandums (see Attachment 5) for all installations until SAF/GC has authorized initiation or continuation of monitoring at all Air Force installations.

1.4.10.2.5. Provides certification cycle guidance and support to MAJCOM, DRU, FOA, and Wing IA offices.

1.4.10.2.6. Reviews, evaluates, and interprets national and DoD notice and consent guidance, and makes recommendations on implementation to SAF/GC, for use in future cycles.

1.4.10.2.7. Works with MAJCOM and DRU A6 office to ensure subordinate installations adhere to established procedures and timelines within this guidance.

1.4.10.2.8. Submit all finalized N&C Summary Reports with endorsements to SAF/GC with courtesy copy to AFSPC/A3 and 24 AF.

1.4.10.2.9. During even-numbered fiscal years, review reports received from each AF installation, ensuring accurate and acceptable reporting of mandatory Notice and Consent actions over the previous 24 months.

1.4.10.2.10. Coordinate required corrective actions identified through the review process with the relevant Wing Information Assurance Office (WIAO).

1.4.11. DELETED

1.4.11.1. DELETED

1.4.11.2. DELETED.

1.4.11.3. Biennially, during even-numbered fiscal years, review reports received from each AF installation, ensuring accurate and acceptable reporting of mandatory notice and consent actions over the previous 24 months.

1.4.11.4. DELETED.

1.4.11.5. DELETED.

1.4.11.6. DELETED.

1.4.11.7. DELETED.

1.4.12. **24th Air Force (24 AF)** will:

1.4.12.1. Direct all worldwide assessment missions.

1.4.12.2. Serve as the focal point for all monitoring requests.

1.4.12.3. Approve all TMAP missions before execution.

1.4.12.4. Oversee the fusion cell.

1.4.12.5. Ensure lessons learned and best practices are submitted through higher headquarters (HHQ) to the AF lessons learned database and AF OPSEC PM.

1.4.12.6. Maintain oversight of standardization and evaluation program.

1.4.12.7. Deploy TMAP forces as the sole Air Force TMAP ~~"f~~force provider" for contingencies

1.4.12.8. Establish standardization and evaluation processes for TMAP operations.

1.4.12.9. Establish a fusion cell within 24th Air Force (24 AF).

1.4.12.10. Authorized to conduct TMAP missions without prior notification on any AF unclassified telecommunication system that has been certified by SAF/GC for consent to monitor.

1.4.12.11. Establish a tasking cell within 24 AF.

1.4.12.12. Perform TMAP activities only at installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

1.4.12.13. Ensure no less than twenty-four 24 AF directed ~~"n~~o-notice" TMAP assessments are conducted across the total number of AF MAJCOMs, DRUs, and FOAs within a fiscal year. These assessments will included at a minimum TMAP telephone, e-mail, and IbC mission subsets.

1.4.13. **The Fusion Cell (**624th Operations Center (624 OC/CPD)) will:

1.4.13.1. Collect and analyze all TMAP products released by units and provide a unified report and identify trends as described in 1.4.9.21 to AFSPC/A3I the 10th day of the following quarter (10 Jan, 10 Apr, 10 Jul, 10 Oct)

1.4.13.2. Periodically request current/updated threat data from NASIC.

1.4.13.3. Distribute the threat data to TMAP units.

1.4.14. **The Tasking Cell** (624 OC/CPD) will:

1.4.14.1. Gain 24 AF/CC approval or receive delegated authority to approve mission tasking.

1.4.14.2. Efficiently task resources to support requests. The Tasking Cell must consider competing objectives when prioritizing requests, maximize the employment of resources, and balance workloads.

1.4.14.3. Schedule TMAP activities only at installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

1.4.14.4. Schedule wireless communications monitoring only when the monitoring equipment is technically capable of isolating monitoring to specific AF telecommunications devices. If the equipment utilized cannot demonstrate clearly and specifically this capability, seek a legal review from 67 NWW/JA before tasking the assessment.

1.4.15. **67th Network Warfare Wing (67 NWW)** will:

1.4.15.1. Identify units authorized to conduct TMAP activities.

1.4.15.2. Ensure ongoing OPSEC vulnerability assessment and comprehensive analysis of content and data traversing/resident on AF owned, leased, and operated IbCs across the full range of military operations is accomplished.

1.4.15.3. In coordination with HHQ, develop and implement procedures to protect the legal rights, civil liberties, and privacy of persons whose communications are subject to assessment.

1.4.15.4. Execute tasked missions through subordinate units.

1.4.15.5. Execute the standardization and evaluation program.

1.4.15.6. Coordinate with and submit TMAP operations resource requirements to HHQ for evaluation and inclusion in AF Program Objective Memorandum process.

1.4.15.7. Submit capabilities shortfalls to HHQ for evaluation and further action.

1.4.15.8. Provide an empirical basis for improving the security of telecommunications against hostile interception.

1.4.15.9. Establish data retention, archival and back-up policies and procedures IAW AFMAN 33-363, Management of Records and AF Records Disposition Schedule at the Air Force Records Information Management System (AFRIMS). Adoption or modification of existing database management best practices will meet this requirement. Destroy nonoperational data as soon as operationally feasible, but no later than 90 days from the issuance of the report for which the information was originally collected. Retain all other mission related data (reports, transcripts, trip reports, site surveys, etc) for 1 year or they are obsolete or no longer needed, whichever is sooner. No raw data may be retained longer than 90 days. EXCEPTION: Any data supporting training requirements may be indefinitely retained provided that the data does not contain any personally identifiable information (PII), or personal privacy information (PPI).

1.4.15.10. Develop a process to mitigate situations when an IbC and/or data monitoring vulnerability assessment reveal information which requires immediate action.

1.4.15.11. The 67 NWW Commander or his/her appointed representative will approve requests for unsanitized transcripts from supported commanders.

1.4.16. **TMAP Units (68 NWS, 352 NWS, and gained reserve units) will:**

1.4.16.1. Comply with this Instruction and HHQ policies/guidance.

1.4.16.2. Perform TMAP activities only at installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

1.4.16.3. Monitor and assess AF telecommunications to satisfy legitimate Information Protection requirements.

1.4.16.4. Identify, capture, store, and evaluate the content of all AF Public and Private web site data including text based, image, audio, and video.

1.4.16.5. Ensure monitoring requests are forwarded through 24 AF to the Tasking Cell for action.

1.4.16.6. Conduct TMAP only on DoD/AF owned or leased telecommunications systems or devices.

1.4.16.7. Monitor official communications only. For example, do not target Class B (on-base quarters) telecommunications.

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

1.4.16.9. Not report or intentionally retain any information regarding acquisition, proprietary, PII, or PPI extraneous to the TMAP assessment. Promptly destroy any such information collected, EXCEPT if it:

1.4.16.9.1. Relates to an intrusion; activities that are likely to significantly impair the efficiency of the system; or activities that are likely to enhance system exposure to intrusions.

1.4.16.9.2. Reveals an emergency threatening serious bodily harm, or significant loss of property.

1.4.16.9.3. Indicates a potential or ongoing serious criminal or counterintelligence concern; such information will be coordinated IAW paragraph 3.2.3 of this Instruction.

1.4.16.9.4. Information identified as potentially privileged: such as confidential communications between attorney and client; psychotherapist and patient; or clergy and person may only be reported after consultation with 67 NWW/JA.

1.4.16.10. Identify non-material solutions to tactical deficiencies by submitting a Tactics Improvement Proposal IAW AFI 11-260, *Tactics Development Program*, to HHQ.

1.4.17. **National Air and Space Intelligence Center (NASIC)** will provide requested threat data to the 67 NWW Fusion Cell for further distribution. This is currently delegated to NASIC OL-A.

1.4.18. **MAJCOM, DRU and FOA Operations Security (OPSEC) Program Managers (PM)** will:

1.4.18.1. Coordinate TMAP requests with 624 OC/CPD (see paragraph 3.1) at the following address **624OC.CPD@lackland.af.smil.mil.**

1.4.18.2. Act as the final arbiter for classification of MAJCOM, DRU, or FOA mission data.

1.4.19. **Wing and Installation Commanders/Directors** will:

1.4.19.1. Send assessment requests to their respective MAJCOM, DRU, or FOA OPSEC PM.

1.4.19.2. Consider using TMAP in appropriate operations and exercise plans.

1.4.19.3. Comply with paragraph 3.2.6 prior to taking disciplinary or administrative personnel action based on TMAP products.

1.4.19.4. Ensure the OPSEC PM or Signature Manager is appointed as the OPR to coordinate the activities of the TMAP team when scheduled to receive an assessment. (See also AFI 10-701) The OPSEC PM or Signature Manager will:

1.4.19.4.1. As required, coordinate with the appropriate network control officials and/or security offices to facilitate the remediation and containment of any classified information identified during the assessment.

1.4.19.4.2. Act as the OPR to coordinate the needs of the assessment team. Assist with assessment preparation. Typical actions are available in Chapter 3.

1.4.19.4.3. Notify the installation Information Protection Officer (IPO) when classified information is involved.

1.4.20. **Installation Legal Offices (JA)** should contact 67 NWW/JA regarding use of TMAP information as evidence prior to advising their commander on supportable disciplinary or other adverse action. 67 NWW/JA will provide a legal review of any proposed use of TMAP products in criminal prosecution or other disciplinary or adverse personnel action to 24 AF/JA and AFSPC/JA, for final coordination with SAF/GCM.

1.4.21. **Organizational IAOs** are responsible for management and execution of the N&C program IAW AFI 33-230, *Commanders Guidance and Responsibilities*, and will:

1.4.21.1. Perform annual self assessments of all information technology to ensure compliance with this guidance using the AF Form 4160 and Chapter 4.

1.4.21.2. Document deficiencies found during the assessment in the Organizational IA detailed report.

1.4.21.3. Correct deficiencies identified within 30 days of the IA assessment.

1.4.21.4. Document and track corrective actions within their IA program to ensure reporting of compliance on the biennial report.

1.4.21.5. Ensure the first pages on all the unit's private/intranet web homepages comply with this guidance. Notice and consent requirements do not apply to public web sites/pages. Pop-ups or links to banners on applicable web sites are not permitted.

1.4.21.6. Submit a biennial report to the Wing IA office (see Attachment 5).

1.4.21.7. Put users of Air Force computer systems, including computers connected to a network, stand-alone computers, and portable (wireless) computers on notice that their use constitutes consent to monitoring by ensuring that each user has a signed AF Form 4394 on file prior to being given access to systems IAW AFI 33-100, *User Responsibilities and Guidance for Information Systems*, and by implementing the notices in Chapter 4.

1.4.21.8. If classified information is found during the course of a notice and consent assessment, then paragraph 3.2.4 of this document applies.

1.4.22. **Training Program Managers**. Upon request, TMAP units may release any mission data subject to the requirements of paragraph 1.14.15.9, this Instruction, to support training programs. Trainers and instructors will:

1.4.22.1. Control access to the recorded communications.

1.4.22.2. Label the recorded telecommunications as containing information obtained through communications monitoring.

1.4.22.3. Inform all students and instructors, in writing, that recorded communications are only for classroom discussion.

1.4.23. **Air Force Space Command, Requirements (AFSPC/A5).** AFSPC/A5 will develop funding documents to procure improved capabilities and ensure maintenance of TMAP capabilities.

1.4.24. **Wing Information Assurance Office (WIAO)** ensure compliance with notice and consent requirements when performing annual IA assessments per AFI 33-230, *Information Assurance Assessment and Assistance Program* and will:

1.4.24.1. Biennially compile a summary letter based on the unit annual reports.

1.4.24.2. Obtain and provide any AFSPC/A6, JA, or GC requested corrections or clarifications.

1.4.24.3. Maintain a copy of the installation's finalized Notice and Consent summary report (See Attachment 5) and SAF/GC Notice and Consent Authorization Memo until the end of the next biennial certification cycle.

Chapter 2

TMAP PRODUCTS

2.1. There are two basic types of TMAP products , consisting of reports and transcripts. Products will not contain PPI, PII, or information that could reasonably identify individuals in assessed offices, flights, or sections, such as titles, names, ranks, complete phone numbers, complete e-mail addresses, etc. Office symbols may be released if the release of the office symbol does not provide sufficient data to identify an individual. A product may contain names, titles, or ranks when it is an integral part of the possible disclosure, unless it somehow identifies one of the monitored parties. EXCEPTIONS: As described in paragraph 3.3.1.

2.2. Products. All TMAP products are at a minimum "FOR OFFICIAL USE ONLY" until possible disclosures are thoroughly evaluated and any weaknesses corrected. Classify TMAP products according to security classification guides, AFI 31-401, *Information Security Program Management*, AFI 24-405, *Department of Defense Foreign Clearance Guide*, and/or the DoD 4500.54-M, *Department of Defense Foreign Clearance Manual*, geographic appendices, and/or classified supplement. Mark products according to current policy and guidance.

2.3. Reports. The four TMAP reports are information protection alerts (IPA), immediate reports, summary reports, and final reports. The customer determines the distribution, frequency, and delivery times of these reports. Reports may include short quotes or extracts of a communication when needed to clarify information presented, but not entire reproductions of communications. Summary and final reports will also include applicable threat information. Samples of IPA, immediate, and summary reports are available in Attachment 2. TMAP reports provide operational commanders and planners with near real-time reports of classified or sensitive information disclosures that may adversely affect US (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.

2.3.1. An IPA is a shortened reporting format used to notify the customer of possible disclosures upon discovery during the assessment. These reports may contain compromises of classified information, information of value to hostile intelligence services, critical information or information pertaining to the movement of high-level distinguished visitors (DV).

2.3.2. An immediate report contains similar information as an IPA, but provides time-sensitive information, force protection information, and mission critical information during exercise and real world operations.

2.3.3. A summary report is a summary of problem areas or possible disclosures noted during the assessment. This report is issued at varying intervals during the assessment, such as monthly, quarterly, or semi-annually. The customer can waive the requirement for this report entirely.

2.3.4. A final report is similar to a summary report, but contains an executive summary (if applicable); recommendations; and all the identified disclosures from the assessment listed in chronological order. This report is typically issued within 30 calendar days after the

completion of the assessment. The customer can grant extensions or waive the requirement for this report entirely.

2.4. Transcripts. A transcript can be part or all of a verbatim reproduction of an assessed communication and may include certain identifying information. It may also contain transcriber's comments or remarks to clarify or enhance understanding of the information presented. There are two types of transcripts -- sanitized and unsanitized.

2.4.1. Sanitized transcripts are furnished upon request to expand on or enhance understanding of information presented in a report. A sanitized transcript is a true representation of a communication, but will not contain personal privacy information (PPI), personally identifiable information (PII), or information that could reasonably identify assessed offices, flights, or sections. They are resource intensive to prepare and should be requested sparingly. Transcripts are typically requested when a report reveals critical information disclosures that may affect operations or possible security violations. Release procedures are specified in paragraph 3.3.

2.4.2. Unsanitized transcripts are true and complete representation of a communication. An unsanitized transcript includes both the sending and receiving communicator's information (if available.)

2.5. Combining Products. Based on evolving information technologies TMAP products may be combined with other products or used within the restrictions of paragraph 3.2.

Chapter 3

TMAP PROCEDURES

3.1. Assessment Request Procedures and Process Flow (See Figure 3 1).

3.1.1. Organizations request assessments through their Wing OPSEC PM to their MAJCOM, DRU, FOA OPSEC PM.

3.1.2. MAJCOM, DRU, and/or FOA OPSEC PMs will actively manage their command's TMAP through directing, soliciting, prioritizing, and consolidating assessment requests. The OPSEC PM will forward request to 624 OC tasking cell which will send these requests to the TMAP unit. At a minimum each MAJCOM and DRU will have two organization requested assessments and FOA will have one organization requested assessment accomplished within a fiscal year. At a These assessments will included at a minimum TMAP telephone, e-mail, and IbC mission subsets.

3.1.3. The Tasking Cell validates and prioritizes requests as follows:

3.1.3.1. Priority 1: Military operations.

3.1.3.1.1. Priority 1A: Major operations and campaigns.

3.1.3.1.2. Priority 1B: Peace operations, crisis response or limited contingency operations.

3.1.3.2. Priority 2: Special Access Programs or Research, Development, Test and Evaluation activities.

3.1.3.2.1. Priority 2A: Existing Special Access Programs.

3.1.3.2.2. Priority 2B: Test and evaluations.

3.1.3.2.3. Priority 2C: Research and development.

3.1.3.3. Priority 3: Air Expeditionary Force pre-deployment exercises or events.

3.1.3.4. Priority 4: AF units participating in Joint Chiefs of Staff directed exercises.

3.1.3.5. Priority 5: Combatant command, MAJCOM, DRU, or FOA exercises.

3.1.3.6. Priority 6: Baseline assessments.

3.1.3.7. Priority 7: All other assessments.

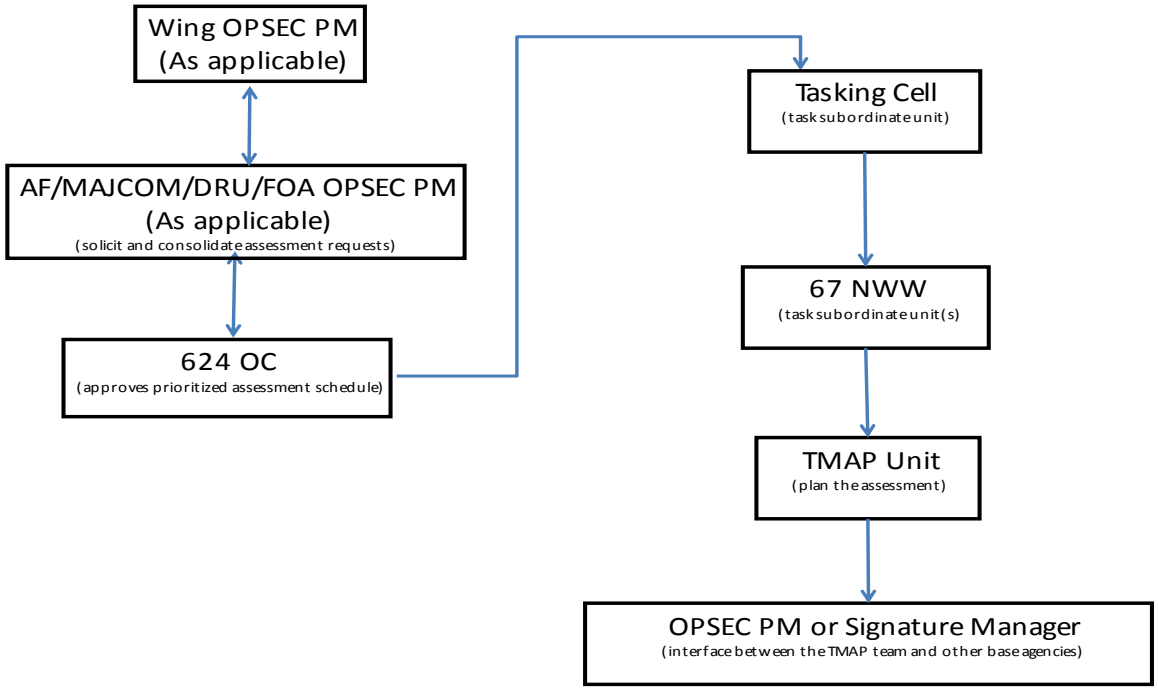
3.1.4. The Tasking Cell will also incorporate threat information when resolving competing or determining overall priorities.

3.1.5. The 24 AF/CC or delegated representative will approve assessment schedules. The approved tasking document constitutes authority for the units to operate.

3.1.6. The Tasking Cell then tasks the 67 NWW to execute the assessments via subordinate units.

3.1.7. TMAP units contact the OPSEC PM or Signature Manager to plan the assessment. Refer to paragraph 3.4 for further details.

Figure 3.1. TMAP Request Process Flow



3.2. Use and Control of Products; Situational Guidance. This section describes the use and control of TMAP products. It also contains specific situational guidance.

3.2.1. All Products. This paragraph applies to all products. This section is applicable and binding to customers, producers of, and anyone who comes into contact with information in these products, without regard to rank, status, or position. Failure to observe the prohibitions and mandatory provisions of paragraph 3.2, and all of its subparagraphs by military personnel is a violation of the *Uniform Code of Military Justice,* Article 92, Failure to Obey Order or Regulation. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contractor personnel will be handled according to local laws and the terms of the contract. All personnel will:

3.2.1.1. Limit distribution of products to the absolute minimum required. The minimum limited distribution required is a copy of all TMAP products to the assessed organizations HHQ OPSEC PM.

3.2.1.2. Protect the rights and privacy of individuals. Protect properly marked proprietary information.

3.2.1.3. Use information in products only for official purposes, except as otherwise noted.

3.2.1.4. Not use products to produce foreign intelligence or counterintelligence information.

3.2.1.5. Release products to Opposing Forces during exercises or evaluations only under the following conditions:

3.2.1.5.1. Reports must maintain their identity as TMAP reports.

3.2.1.5.2. Do not identify or represent the products to be as signals intelligence.

3.2.1.5.3. Do not identify any communicating parties

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

3.2.2. Emergency situations. This paragraph will apply if information threatening death, serious bodily harm, significant or intentional compromise of classified information, or major loss of property is obtained during the assessment.

3.2.2.1. Immediately report this information, as appropriate, to the military commander; Air Force Office of Special Investigations (AFOSI); US law enforcement agency having jurisdiction of the assessed unit; or other agency as necessary to resolve the emergency.

3.2.2.2. Use the most expeditious means of reporting that provides full security.

3.2.2.3. Complete identifying data may be released.

3.2.2.4. This is not a TMAP product; therefore, the information will not appear in a TMAP product.

3.2.2.5. Immediate action may be taken by appropriate authorities to address the emergency situation.

3.2.2.6. Until properly reported, the emergency situation has priority. Resources may be re-assigned and other assessment missions may be suspended or delayed as necessary.

3.2.2.7. Within 24 hours of initial reporting, notify 67 NWW/JA, by message, with copies to HHQ.

3.2.3. Criminal Information. Except potentially privileged communications related to personal representation or services by attorneys, psychotherapists or clergy, and their assistants and between husband and wife, information incidentally acquired during TMAP activities that directly relates to a significant crime shall be reported as follows:

3.2.3.1. Immediately report this information to the unit commander and AFOSI.

3.2.3.2. Complete identifying data may be released.

3.2.3.3. This is not a TMAP product; therefore, the information will not appear in a TMAP product.

3.2.3.4. Within 24 hours of initial reporting, notify 67 NWW/JA, by message, with copies to HHQ/JA. 67 NWW/JA will promptly provide a legal review of the report to be forwarded via command JA channels to AF/JAO and SAF/GCM.

3.2.4. Classified information. This paragraph will apply if information revealing a compromise or continuing threat of a compromise of classified information is obtained during the assessment. Follow guidance within AFI 31-401, *Information Security Program Management* and/or AFI 33-138, *Enterprise Network Operations Notification and Tracking,* Chapter 6. If found within an assessed communication also:

3.2.4.1. Release only the minimum amount of data necessary to ensure prompt remedial action. Briefly summarize what was sent and its classification.

3.2.4.2. If an attachment is present, it may also be sent using secure means to the appropriate IPO, OPSEC PM, or Signature Manager for evaluation. The IPO is the first level of management for classified information.

3.2.4.3. Release full header information (to, from and cc lines or sending/receiving addresses; dates/times; and subject line) or account information (enclave, username and password) to the appropriate network control officials, security offices, OPSEC PM, or Signature Management POC to facilitate the positive identification, containment, and remediation of compromised data or account from the network or information system.

3.2.5. DV movements. The following information, if encountered during an assessment, must be properly reported IAW AFI 71-101, Volume 2, *Protective Service Matters*, and included in a product:

3.2.5.1. High-level DV movements, such as the President, Vice President, foreign heads of state or foreign ambassadors. Report this information to the local AFOSI detachment at the location of the assessment.

3.2.5.2. Classify products utilizing AFI 31-401, AFI 24-405, and/or DoD 4500.54-M*, Department of Defense Foreign Clearance Manual* for overseas travel or security classification guide for the theater, mission or operation. Specific itineraries may carry a higher classification based on trip sensitivity. For information regarding classification guides contact the IPO.

3.2.6. Adverse or disciplinary personnel actions. Failure to observe the prohibitions and mandatory provisions of paragraph 3.2, and all of its subparagraphs by military personnel is a violation of the UCMJ*,* Article 92, *Failure to Obey Order or Regulation*. Violations by non-federalized ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Information obtained during an assessment will not be used as evidence in a criminal prosecution without approval of SAF/GC. Prior to drafting charges, installation level SJAs shall submit TMAP derived materiel they intend to use as evidence to 67 NWW/JA for comment. 67 NWW/JA's legal review shall be provided via command JA channels to AF/JAO, AF/A3Z-C and SAF/GCM for coordination.

3.2.7. Awareness and training. TMAP products can support Information Protection awareness and training efforts by providing real-world examples of exposed information and communications practices.

3.2.7.1. TMAP units may provide extracts of reports and brief quotes of assessed communications. Communicating parties will not be identified in any way.

3.2.7.2. Readily available and relevant statistics may also be provided. They will not be interpreted to rank or compare any MAJCOM, DRU, FOA, base, wing, group, squadron, section, flight, or unit.

3.2.8. Vulnerabilities to Unclassified Government Owned/Leased Networks and Databases. Follow guidance within AFI 33-101, *Commanders Guidance and Responsibilities* and/or AFI 33-138, *Enterprise Network Operations Notification and Tracking*, Chapter 5.

3.2.8.1. If found within an assessed communication also follow guidance of this Instruction, paragraph 3.2.6.1. Release full header information (to, from and cc lines or sending/receiving addresses; dates/times; and subject line) or account information (enclave, username, and password) to the appropriate network control officials, security offices, OPSEC PM , or Signature Manager to facilitate the positive identification, containment, and remediation of compromised data or account from the network or information system.

3.3. Transcript Release Procedures. Sanitized transcripts are released upon request from the assessed installations OPSEC PM/Signature Management POC. Electronic means are preferred, but telephonic or written requests will also be honored. Sanitized transcripts must be requested within 45 work days from receipt of the TMAP report. Contact the unit providing the report.

3.3.1.1. The assessed organization commander/director has determined that a security violation has occurred and request through their HHQ OPSEC PM an unsanitized transcript.

3.3.1.2. The HHQ OPSEC PM of the assessed organization will review, coordinate on, and forward the request for an unsanitized transcript to 67 NWW for action.

3.3.1.3. 24 AF/A3 will review the request, if warranted request the unsanitized transcript from the TMAP unit that conducted the assessment, review the unsanitized transcript, and consult with 24 AF/JA. Legal offices supporting the requestor may consult with 24 AF/JA regarding the request to ensure the legal analysis fully considers the concerns of the requestor.

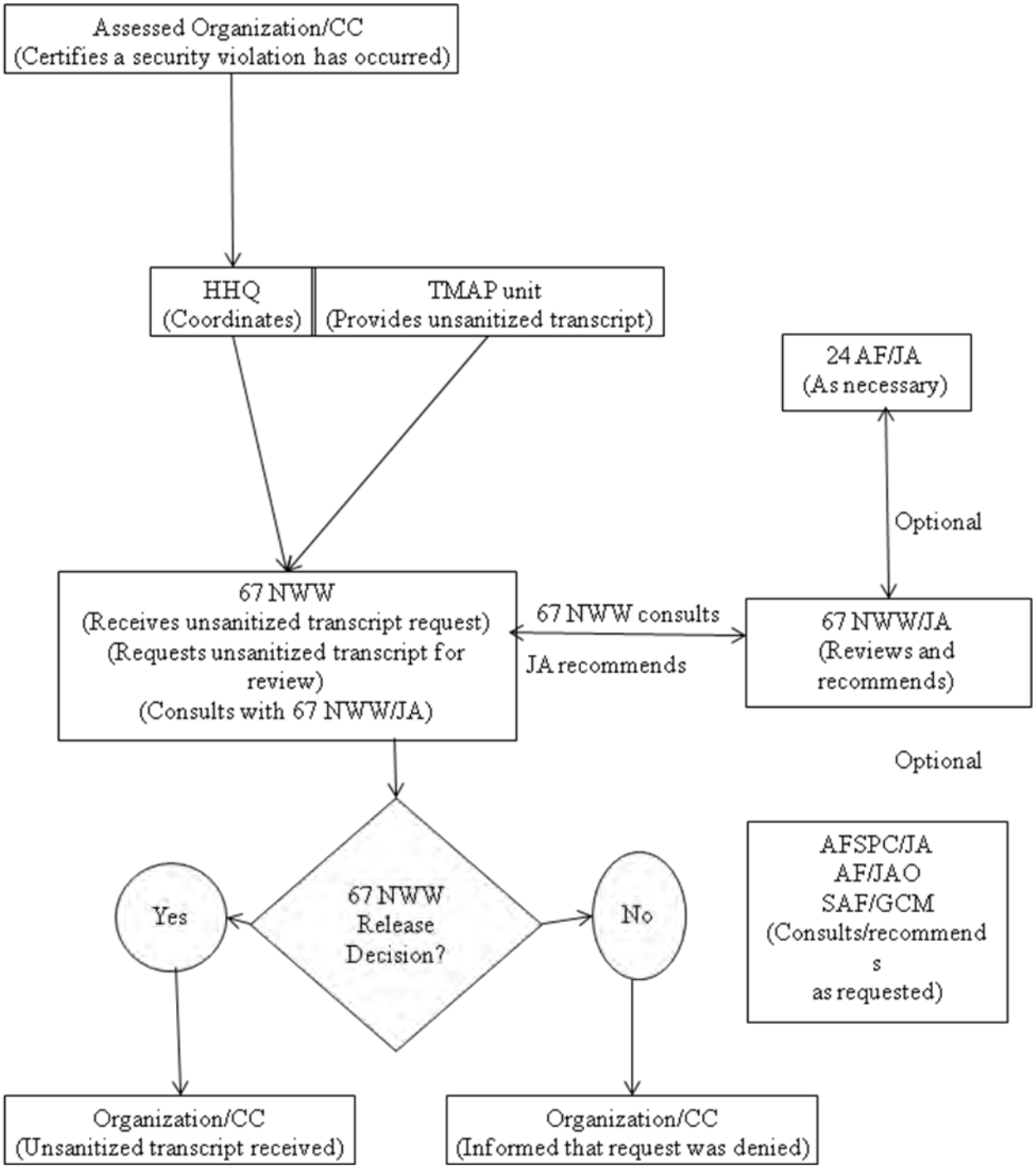
3.3.1.4. If the 67 NWW Commander determines the release of the names and other identifying data is justified, he/she will forward the unsanitized transcript as requested. If disapproved, he/she will notify the requesting organization.

3.3.1.5. 67 NWW Commander may only provide unsanitized transcripts to requesters authorized to review them under the guidelines established above or in accordance with other statutes, executive orders, or DoD policies. Unsanitized transcripts may not be released without approval from SAF/GC.

3.3.1.6. In the case of failure to follow directed OPSEC countermeasures and/or unauthorized disclosure of critical information by personnel who are not members of the tasked or requested assessment unit; TMAP personnel are authorized to release disclosure details to their commanders/directors or appointed representative.

3.3.1.7. If commanders and or directors feel a violation has occurred they can initiate a request for a sanitized or unsanitized transcript via procedures detailed in paragraph 3.3.

Figure 3.2. Unsanitized Transcript Process



3.4. Team Support. TMAP teams will require assistance from the assessed organization well before the actual start date of the assessment. The OPSEC PM or Signature Manager is usually tasked to interface between the TMAP team and other base agencies. The following are typical actions to prepare for an assessment, but not all-inclusive:

3.4.1. Gain familiarity with TMAP objectives and methods.

3.4.2. Coordinate a work area and secure storage facility for the TMAP team.

3.4.3. Assist the team with arrangements for billeting, transportation, and messing.

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

3.4.5. If necessary, arrange funding for local telephone exchange connection fees.

3.4.6. Ensure senior leadership is advised of TMAP activities.

3.4.7. Ensure administrative communication capabilities are available to teams for operational or administrative support. Arrange specialized communications support as needed to meet mission requirements.

3.4.8. Upon request, provide operational orders, plans, operating instructions, security classification guides, phone directories, or other mission related documents.

3.4.9. Generate an initial list of phone numbers to be assessed (approximately 125-200). Use sound judgment in the creation of the list. Functions, flights, offices, or sections should be considered for assessment based on roles or contribution to the mission or operation. Medical facilities, legal offices, and chapels/chaplains will not be selected for assessment.

3.4.10. Determine product distribution listing (who), product delivery time and frequency (when/how often), and pass to the assessment team.

Chapter 4

NOTICE AND CONSENT PROCEDURES

4.1. Notification. Users of DoD telecommunications devices are to be notified the use of DoD telecommunications systems constitutes consent to monitoring. Notification procedures in this Instruction are ***mandatory*** for official DoD information technology to include but not limited to telecommunications systems and devices.

4.2. 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."

4.2.1. This banner is required to be displayed on the first page of electronic versions of the telephone directory.

4.2.2. For the purpose of Notice and Consent, unofficial organizational charts and rosters are not considered telephone directories.

4.3. Telephones. Affix DD Form 2056, *Telephone Monitoring Notification Decal***,** on the front of all official telephones. For telephones with secure voice capability that can be used in the unsecure mode, such as Secure Terminal Equipment (STE), etc., remove the words **"DO NOT DISCUSS CLASSIFIED INFORMATION"** from the form. When the DD Form 2056 cannot be placed on the front of a phone, place on side nearest the user's view. Replace the DD Form 2056 when wear and tear prevents reading of the complete notice and consent statement. Locally recreated Notice and Consent stickers are permitted as long as the wording matches the DD Form 2056 exactly.

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

4.4.1. Affix DD Form 2056, on all facsimile machines.

4.4.2. Use the AF Form 3535, or, if using a local facsimile cover sheet, include the exact notice and consent statement cited below:

"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."

4.5. Information Systems. Put users of Air Force computer systems, including computers connected to a network, stand-alone computers, and portable (wireless) computers on notice that their use constitutes consent to monitoring.

4.5.1. Install the notice and consent log-on banner, Attachment 3, 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.

4.5.2. For information systems where it is not technically feasible (due to character limitations, etc.) to install the complete notice and consent log-on banner cited in Attachment 3, as determined by the MAJCOM or DRU/A6, perform the following requirements:

4.5.2.1. Install the abbreviated log-on banner cited below on the information system:

"I've read & consent to terms in IS user agreem't."

4.5.2.2. Ensure users of the system have a valid AF Form 4394 on file. The signed forms will be retained by the organizational IAO or designated representative until six months after the user no longer requires access to the system.

4.5.2.3. If the system is not capable of complying with paragraph 4.5.2.1, DD Form 2056, or another label worded exactly the same, must be affixed on all computer monitors or video display screens of those information systems.

4.6. Private or Intranet Web Homepages. Prominently display the exact notice and consent banner specified in Attachment 3 on the first page of all private and intranet web homepages; the banner is not required on subsequent pages. Pop-up screens or hyperlinks to the notice and consent statement do not meet the requirement as it pertains to private/intranet web pages.

4.6.1. Notice and consent requirements do not apply to public web pages. Refer to AFI 33-129, Web Management and Internet Use, for privacy and security notice requirements for public web pages.

4.6.2. Applications. The DoD Banner/User Agreement policy memorandum only applies to DoD information systems, not applications. If an information system is configured such that first access is through an application, then the notice and consent banner is required or the information system would need to be configured to present the notice and consent banner prior to accessing any applications.

4.7. Portable Electronic Devices (PED). A PED is any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information (e.g. text pagers, personal digital assistants, cellular telephones, and hand-held radios/land mobile radios (LMRs)). Refer to Air Force System Security Instruction (AFSSI) 8502, *Organizational Computer Security*, for more information on PEDs. For a more complete list, see definition in Attachment 1. These devices must comply with the requirements in paragraph 4.5. except as noted below:

4.7.1. When a device is issued, all receiving personnel must 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."** Due to size of the devices and OPSEC concerns, labeling PEDs with the DD Form 2056 is optional and at the discretion of the organization IAO.

4.7.2. Exception: For Hand-held radios/LMRs:

4.7.2.1. Label hand-held radios/LMRs with the DD Form 2056 unless the organization commander has OPSEC concerns based upon the local operating environment. See AFI 10-710 for OPSEC risk management procedures.

4.7.2.2. If the commander has OPSEC concerns and does not direct use of the DD Form 2056, personnel must sign a form that includes the following notice and consent statement for use of the device: **"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."**

4.7.3. All signed Wireless PED User Agreements will be retained by the Organizational IAO or the designated representative for a minimum of six months after the device has been returned to the issuing office.

4.8. Other Information Technology. Any telecommunication devices not otherwise referenced in this chapter must have a signed user agreement 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 Organizational IAO or the designated representative for a minimum of 6 months after the device has been returned to the issuing office.

4.9. Optional Notice and Consent Awareness Methods. Optional methods are not to be included in notice and consent packages. Use of any or all optional methods listed below will not substitute for methods listed as mandatory. Optional methods to provide users with legally sufficient notice their use of telecommunications and information systems constitutes consent to monitoring for authorized purposes is outlined as follows:

4.9.1. Correspondence from the base or facility commander, addressing notice and consent provisions, to all assigned units for dissemination to unit personnel.

4.9.2. Addressing notice and consent provisions to newcomers during in-processing, periodic operations security, (OPSEC) awareness briefings, and commander's calls.

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

4.9.4. Incorporating notice and consent provisions in operating procedures, instructions, information system security rules of behavior or acceptable use guidance, etc., that are periodically reviewed by users.

4.9.5. 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.

NOTICE AND CONSENT BIENNIAL CERTIFICATION PROCESS

4.10. Certification Process. This section describes the biennial certification, through the SAF/GC, that users of Air Force telecommunications systems and information systems are provided legally sufficient notice that use of those systems constitutes consent to monitoring for all authorized purposes. This process ensures SAF/GC reviews and provides written approval of Air Force telecommunications monitoring and IA readiness testing procedures, training processes, and user notification procedures on a biennial basis, as mandated by DoDI 8560.01.

4.10.1. AFSPC/A6, initiates the Biennial Notification Process by sending out a task message to the MAJCOM, DRU, and FOAs with the certification schedule.

4.10.2. 24 AF will release annual Cyberspace Tasking Orders (CTO) mandating compliance with the use of Department of Defense (DoD) Standard Notice and Consent Banner and User Agreement statements.

4.10.3. Wing IA Offices will at a minimum, complete and document the actions outlined in this guidance.

4.10.3.1. Prepare a detailed summary of the previous 24-month notice and consent actions following standards described in this guidance. The Wing IA office sends this summary to the installation SJA by *15 April* of each even-numbered fiscal year. The template for the summary letter is provided in Attachment 5.

4.10.3.1.1. The Notice and Consent Checklist Attachment 6, will determine which attachments are required in the N&C summary package.

4.10.3.1.2. The Wing IAO should ensure FOA, DRU, GSU, and tenant packages are in compliance before host package is submitted. Note that attachments and summary letters for FOAs, DRUs, GSUs, and tenants should not be included in the package. List all GSU, FOA, DRU, and other tenants in paragraph #1 of the Notice and Consent Memorandum (See Attachment 5).

4.10.3.1.3. Submit summary packages electronically in PDF format with either ~~"~~wet" ink or digital common access card (CAC) enabled signatures for all required endorsements.

4.10.3.2. Summary letters covering more than one physical installation (example: remote Air Base as a GSU) must clearly identify each installation. FOAs DRUs and tenants will be addressed per the following:

4.10.3.2.1. FOA and DRU located on a host base will report their Notice and Consent compliance through the host Wing IA office.

4.10.3.2.2. FOA and DRU not located on a host base will report their Notice and Consent compliance as a Wing IA office.

4.10.3.2.3. All other tenant wings or organizations report their Notice and Consent compliance through the host installation Wing IA office.

4.10.4. Following host base wing or communications commander signature, installation SJA endorsement and MAJCOM or DRU /SJA endorsement, the Wing IAO sends the installation summary package, with supporting documentation for review no later than 15 May. Wing IAOs also send an informational copy of only the summary letter to the MAJCOM and DRU/A6.

4.10.5. The Installation Staff Judge Advocates (SJA) reviews the summary and attached documentation and provides written review (see Attachment 5 for SJA 1st endorsement format). This SJA review should ensure the actions taken are sufficient to establish

compliance with the requirements of this Instruction. The summary and its attachments should clearly demonstrate users of DoD telecommunications or information systems know such use constitutes consent to monitoring. If the SJA determines the documentation is deficient in any of the requirements, the package shall 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 certification package. Upon endorsement, the installation SJA shall forward the summary back to the Wing IA Office for their tracking and submission to the MAJCOM or DRU SJA for endorsement. Final submissions to MAJCOM and DRU SJA must occur NLT 1 May.

4.10.6. MAJCOM /A6 , in coordination with AFSPC/A6, ensures subordinate bases and installations adhere to established procedures and timelines within this guidance as well as respond to all summary report requests for correction or clarification within 14 duty days.

4.10.7. MAJCOM SJA reviews the summary, attached documentation for legal compliance, and provides written review (see Attachment 5 for MAJCOM SJA 2nd endorsement format). If the MAJCOM SJA determines the documentation is deficient in any of the requirements, the package shall be returned for corrective action. If the package is determined to be legally sufficient, the MAJCOM SJA's written determination becomes part of the certification package. The MAJCOM SJA returns the package to the Wing IA.

4.10.8. AFSPC/JA approves all summary packages before submission to SAF/GC.

4.10.9. Any deficiencies noted by AFSPC/JA are submitted to the Wing IAO. When necessary for compliance, coordination through the MAJCOM is required to ensure installations understand and accomplish necessary corrective actions. Once deficiencies are sufficiently addressed, corrected packages are reviewed by AFSPC/JA.

4.10.10. AFSPC/A6 ensures all Air Force facilities submit inputs in order to receive biennial certification according to Table 4.1, Notice and Consent Certification Schedule. Sends the AFSPC/JA approved package with AFSPC/JA endorsement to SAF/GC, 1740 Air Force Pentagon, Suite 4C756, Washington, DC 20330-1740, by *15 July*. If AFSPC/JA or SAF/GC determines a summary contains insufficient evidence of Notice and Consent actions as required by this Instruction, the Wing IA and Wing/JA will be notified to provide follow-on corrective action, with MAJCOM/A6 and MAJCOM/JA included as information addressees on the notification. AFSPC/A6 will collect process metrics where possible, monitor, and report processing times to AF/A3/A5, SAF/CIO A6, SAF/GC, and MAJCOM.

4.10.11. SAF/GC certifies that there has been sufficient notice that the use of DoD telecommunications and information systems constitutes consent to monitoring. If SAF/GC determines the summary package contains insufficient evidence to establish full compliance with notice of monitoring requirements, the summary is returned for further corrective action prior to certification. Once all base summary reports contain legally sufficient actions for notice and consent, SAF/GC returns a certification listing to AFSPC/A6 by 1 September of each even-numbered fiscal year listing all installations approved for authorized monitoring activities. Upon receipt of the certification listing, AFSPC/A6 will forward copies to an authorized monitoring agency as prescribed by DoDI 8560.01. AFSPC/A6 will forward copies of the certification listing to 624 OC on or before 25 September of each even number fiscal year. Any updates to the certification listing will be forwarded to 624 OC immediately

upon receipt. This certification listing is valid for two years, expiring on 30 September of the next even numbered year.

4.10.12. DELETED.

4.11. Notice and Consent Certification Schedule. Table 4.1. outlines the biennial notice and consent certification schedule of suspense dates and timelines.

Table 4.1. Notice and Consent Certification Schedule

Even Year Date	Office	Action
Mid-January	AFSPC/A6	Release heads-up message to MAJCOM, DRU, FOA/A6s announcing start of certification cycle
Early February	AFSPC/A6	Conduct telecon w/MAJCOM, DRU, FOA/A6s and Wing IA Offices - Initiates Biennial Notification Process
Early February	AFSPC/A6	(If necessary) If new procedures and guidance is required issue a General Guidance Memorandum with Report Template to all Wing IA Offices with courtesy copy to MAJCOM, DRU, FOA/A6s
Early February - After Telecon	AFSPC/A6	Release Notice and Consent Kick-off Message to MAJCOM, DRU, FOAs
Early February	624 OC	Issues CTO on required use of DoD Standard Notice and Consent Banner text
15 Apr – 1 May	Wing IA Office / Installation JA	Sends Notice and Consent Certification Package Summary to Installation SJA for review. Sends endorsement to Wing IA Office.
1 May – 15 May	Wing IA Office / MAJCOM JA	Sends Notice and Consent Certification Package Summary to MAJCOM SJA for review. Sends endorsement to Wing IA Office.
Before 15 May	Wing IA Office	Submits Package Summary for review
15 May	Wing IA Office	Notify MAJCOM, DRU, FOA A6 that package was submitted for review
15 May – 15 July	AFSPC/A6	Reviews Package Summary, addresses any corrections required to WIAO, sends reviewed packages to AFSPC/JA for review and approval
15 May – 15 July	AFSPC/JA	Identifies any corrections required; sends endorsement to AFSPC/A6.
15-Jul	AFSPC/A6	Consolidates package and sends AFSPC/JA endorsement with reviewed package to SAF/GC with courtesy copies

		to AFSPC/A3 and 24 AF
1-Sep	SAF/GC	Provide AFSPC/A3 with a list of bases approved to continue monitoring - Messages received as bases are approved
15-25 Sep	AFSPC/A6	Releases messages listing certified bases

HERBERT J. CARLISLE, Lt Gen, USAF
DCS, Operations, Plans & Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD 4500.54-M, *Department of Defense Foreign Clearance Manual*, 19 February 2009

DoDD 5205.02, *Operations Security (OPSEC) Program,* 6 March 2006

DoDI 8500.2, *Information Assurance Implementation*, 6 February 2003

DoDI 8560.01, *Communications Security (COMSEC) and Information Assurance (IA) Readiness Testing*, 9 October 2007

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010

AFPD 10-7, *Information Operations*, 6 September 2006

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

AFI 10-701, *Operations Security*, 18 October 2007

AFI 11-260, *Tactics Development Program*, 12 December 2003

AFI 24-405, *Department of Defense Foreign Clearance Guide*, 6 May 1994

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

AFI 33-100, *User Responsibilities, and Guidance for Information Systems*, 19 November 2008

AFI 33-101, *Commanders Guidance and Responsibilities,* 18 November 2008

AFI 33-129, *Web Management and Internet Use,* 3 February 2005

AFI 33-200, *Information Assurance Management*, 23 December 2008

AFI 33-230, *Information Assurance Assessment and Assistance Program*, 4 August 2004

AFI 71-101, Volume 2, *Protective Service Matters*, 18 November 2002

AFMAN 33-363, *Management of Records*, 01 March 2008

AFSSI 8502, *Organizational Computer Security*, 18 September 2008

Adopted Forms

DD Form 2056, *Telephone Monitoring Notification Decal*

AF Form 847, *Recommendation for Change of Publication*

AF Form 3535, *Facsimile Electro Mail Transmittal*

AF Form 4394, *Air Force User Agreement Statement – Notice and Consent Provision*

AF Form 847, *Recommendation for Change of Publication*.

Abbreviations and Acronyms

AF—Air Force (when used on forms)

AFSSI—Air Force System Security Instruction

ANG—Air National Guard

AFNIC—DELETED

AFR—Air Force Reserve

COMSEC—Communications Security

DCI—Defense Critical Infrastructure

DoD—Department of Defense

DRU—Direct Reporting Unit

DTS—W - Defense Telecommunications Service-Washington

FOA—Field Operating Agency

GSU—Geographically Separated Unit

IA—Information Assurance

IAAP—Information Assurance Assessment and Assistance Program

IbC—Internet-based Capability

IP—Information Protection

IPA—Information Protection Alerts

JCMA—Joint COMSEC Monitoring Activity

LMR—Land Mobile Radio

MAJCOM—Major Command

NASIC—National Air and Space Intelligence Center

OPSEC—Operations Security

PDA—Personal Digital Assistant

PED—Portable Electronic Device

PII—Personally Identifiable Information

PM—Program Manager

PPI—Personal Privacy Information

RDS—Records Disposition Schedule

STE—Secure Terminal Equipment

STU—III - DELETED

TMAP—Telecommunications Monitoring and Assessment Program

WIAO—Wing Information Assurance Office

Terms

Note: For brevity, terms available in JP 1—02 are not repeated here.

Customer—The requesting organization or the Air Force unit identified to receive an assessment.

Homepage— A starting point or center of an infrastructure on the WWW. A typical home page will consist of hypertext links (hyperlinks) to other Web documents.

Hyperlink— A way to link access to information of various sources together within a Web document. A way to connect two Internet resources via a simple word or phrase on which a user can click to start the connection. Also referred to as a ―link.‖

Information Assurance (IA)— Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Protection— The collective policies, processes, and implementation of risk management/mitigation actions instituted to prevent the loss, compromise, unauthorized access/disclosure, destruction, distortion, or inaccessibility of information, regardless of the physical form or characteristics, over the life cycle of the information. It includes actions to regulate access to sensitive information, controlled unclassified information, and classified information produced by, entrusted to or under the control of the United States Government.

Intranet— A private network that works like the Web, but is not on it. Usually owned and managed by an organization.

Land Mobile Radio (LMR)— A hand held ―walkie-talkie‖ type radio; an LMR is one type of PED (see below).

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

Personnel Action— Any action taken on a member of the armed forces or a Government civilian employee that affects or has the potential to affect that member's current position or career. Such actions include (but are not limited to Promotions, demotions, disciplinary action, corrective action, transfer, reassignment, or significant change in duties or responsibilities inconsistent with rank. (*AFI 90-301*)

Personal Digital Assistant (PDA)— Devices such as Palm Pilot®, Cassiopeia®, Blackberry®, etc.; a PDA is one type of PED (see below).

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

Pop—up Screen — A screen that automatically displays, often prior to entering a web site or accessing a system; normally users must close or acknowledge the pop-up before proceeding further. **Portable Electronic Device (PED) —** Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is

not limited to PDAs, cellular/PCS phones, two-way pagers, email devices, audio/video recording devices, and hand-held/laptop computers [DoDI 8100.2].

Private Web Page— Web pages intended for viewing by a limited audience, specifically .mil and .gov users; distinct from web pages intended for viewing by the general public.

Privilege— A claim of privilege includes, but is not limited to, the assertion by any person of a privilege to: (1) Refuse to be a witness; (2) Refuse to disclose any matter; (3) Refuse to produce any object or writing; or (4) Prevent another from being a witness or disclosing any matter or producing any object or writing. (*Manual for Courts-Martial*)

Sanitized Transcript— A verbatim reproduction of an assessed communication, except it will not contain information that could reasonably identify the communicating parties, such as titles, names, ranks, phone numbers, complete e-mail addresses, office symbols, or duty sections. Transcripts may also contain transcriber's comments or remarks to clarify or enhance understanding of the information presented.

Secure Terminal Equipment (STE)— A type of secure telephone unit; a STE can be used for classified voice or facsimile transmission.

Secure Telephone Unit, Third Generation (STU—III) — DELETED

Significant Crime— A serious offense punishable under the authority of the Uniformed Code of Military Justice or other applicable law by death or by confinement for a term exceeding 1 year. (*Manual for Courts-Martial*, paragraph 95(c) (2))

Summary Package—- Collection of the previous 24 month notice and consent actions showing compliance with the biennial certification requirement that users of Air Force telecommunications systems and information systems are provided legally sufficient notice that use of those systems constitutes a consent to monitoring.

Transcript— A transcript can be part or all of a verbatim reproduction of an assessed communication and may include certain identifying information. It may also contain transcriber's comments or remarks to clarify or enhance understanding of the information presented. There are two types of transcripts – sanitized and unsanitized.

Unsanitized Transcript— Is a verbatim reproduction of an assessed communication including any indentifying information. It includes both the sending and receiving communicator's information (if available.)

Unsecured— Communications that do not use authorized cryptographic products or protected distribution systems.

Attachment 2

SAMPLE TMAP REPORTS

Note: These are provided as samples of TMAP reports, and are not binding or absolute. Variations in format and/or content are authorized.

Figure A2.1. Sample Information Protection Alert

INFORMATION PROTECTION ALERT		
THE INFORMATION IN THIS ALERT WILL BE USED ONLY FOR OFFICIAL US GOVERNMENT PURPOSES		
Classification: UNCLASSIFIED	Mission # : ET 017-09	Alert # : 1
Organization: HQ ACC	Purpose: Routine/Baseline Assessment	Date: 13 Apr 2009
Category:	C4I Network Configuration and Critical Node Information	
POC and Phone #:	SSgt Sharptack, DSN 312-240-xxxx	
Disclosure: The actual meat and potatoes of the IPA will be here…		

UNCLASSIFIED

Figure A2.2. Sample Immediate or Summary Report

UNCLASSIFIED

DEPARTMENT OF THE AIR FORCE
67TH NETWORK WARFARE WING (AFSPC)
467 MOORE ST
SAN ANTONIO TX 78243-7135

11 November 2009

MEMORANDUM FOR CUSTOMER

From: ESSAC Mailing Address
XXXXXX
XXXXXX

Subject: Immediate ESSA Report #1, Supported Activity, Location(s), Task XXX-XX (U)

THE INFORMATION IN THIS REPORT WILL BE USED ONLY FOR OFFICIAL U.S. GOVERNMENT PURPOSES (U)

1. (U) Disclosure specifics. ANALYST COMMENT: *Include if warranted.* (Source: Two local telephone calls on Ramstein AB GE on 110900Z and 120800Z Nov 09. Probability of Intercept: Low. Impact level: High)

2. (U) **Classification and POC Information.** If, after review, you have any questions regarding this report or any item(s) warrants a change in classification, please contact POC XXXXX at DSN XXX-XXXX (STU-III capable) or SIPRNet address.

//SIGNED//
JOHN A. DOE, TSgt, USAF
Mission Supervisor

Classified By:
Classification Reason:
Declassify On:

UNCLASSIFIED

Attachment 3

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

A3.1. [Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]

A3.2. You are accessing a U. S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

A3.3. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

A3.3.1. The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

A3.3.2. At any time, the USG may inspect and seize data stored on this IS.

A3.3.3. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

A3.3.4. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

A3.3.5. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

*OK

A3.4. [For Blackberries and other PDAs/PEDs with severe character limitations:]

****I've read & consent to terms in IS user agreem't.**

Attachment 4

MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

A4.1. By signing this document you acknowledge and consent that when you access Department of Defense (DoD) information systems:

A4.2. You are accessing a U. S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

A4.3. You consent to the following conditions:

A4.4. The U. S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

A4.5. At any time, the U. S. Government may inspect and seize data stored on this information system. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

A4.6. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

A4.7. Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

A4.8. Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications.

A4.9. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

A4.10. Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD direction. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

A4.11. Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy direction.

A4.12. A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD direction. However, in such cases, the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

A4.13. These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

A4.14. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD direction, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

A4.15. All of the above conditions apply regardless of whether the access or use of an Information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this user agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this user agreement.

Attachment 5 (Template)

NOTICE AND CONSENT MEMORANDUM WITH 1ST AND 2ND IND

Figure A5.1. Notice And Consent Memorandum with 1st And 2nd Ind

MEMORANDUM FOR: [Supporting Legal Office]

FROM: [XX CS]
[Anywhere AFB 12345]

SUBJECT: Summary of Consent Notification Actions Taken During the Two-Year Period From 1 Apr xx - 31 Mar xx

1. The following actions were taken during the past two years to notify users of DoD telecommunications systems and devices that using telecommunications systems and devices constitutes consent to telecommunications monitoring for Anywhere AFB (and the following Geographically Separated Units, Tenants, Field Operating Agencies, and Direct Reporting Units: [list]).

a. The current base telephone directory, dated_____, includes the notice and consent statement from AFI 10-712, Paragraph 4.2, on the front cover, or on first page of the official portion of the phone book. 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 (AFI 10-712, Paragraph 4.3).

b. All telephones were inspected on [date] and XX% of all phones had the DD Form 2056, Telephone Monitoring Notification Decal, affixed. 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 facsimile machines were inspected on [date] and XX% of all machines had the DD Form 2056 affixed. Decals were immediately applied to all noncompliant fax machines. Consequently, all faxes have DD Form 2056 affixed as of the date of this report. All personnel use the AF Form 3535 or another cover sheet that includes the statement in paragraph 4.4.2. Screen prints of all locally produced fax cover sheets are attached.

d. On [date], it was verified all individuals issued an official Portable Electronic Device (PED) including, but not limited to, cell phones, Personal Digital Assistants (PDA), and text pagers have signed a receipt which includes the notice and consent statement from AFI 10-712, Paragraph 4.7.1. Additionally, hand-held radios/LMRs have the DD Form 2056, Telephone Monitoring Notification Decal affixed or a signed acknowledgment of notice and consent according to AFI 10-712, paragraph 4.7.2. Consequently, XX% of all PEDs are notice and consent compliant.

e. The exact notice and consent banner as mandated by DOD Directive Type Memorandum (DTM) 08-060, Policy on Use of Department of Defense (DoD) Information Systems, Standard

Consent Banner and User Agreement has been installed on all information systems including, but not limited to, computers connected to a network, servers, stand-alone computers, portable computers, switches, and routers. The banner is automatically displayed upon boot-up or initial log-on for the information system regardless of the method accessed (see attach. 1). All computers were inspected and XX% of all computers displayed the log-on banner. The banner was immediately installed on all non-compliant computers. Consequently, all information systems display the log-on banner as of the date of this report.

f. The current notice and consent banner is prominently displayed on the first page of all of the unit's private/intranet web homepages. The warning banner is worded exactly as the log-on banner mandated in AFI 10-712, Attachment 3. Screen prints of all private web homepages page are attached.

g. Other notification actions: (List any optional notice and consent awareness methods (AFI 10-712, Paragraph xx) used to notify installation personnel.)

2. My POC for this issue is [Name, Rank, Org/Ofc, DSN xxx-xxxx, Commercial (xxx) xxx-xxxx].

I.M. TALKER, Lt Col, USAF
Commander (Communications Squadron)

6 Attachments:
1. Telephone Directory Front Cover or First Page of Official Portion of Telephone Directory
2. Print Screen of Electronic Telephone Directory Web Page
3. Copy of Locally Produced FAX Cover Sheet (if used)
4. Copy of Portable Electronic Device (PED) User Agreement
5. Print Screen of Information System Notice and Consent Banner
6. Print Screen of Unit Private Web Pages with Notice and Consent Banner

1st Ind, JA xx Apr xx

TO: 123d CS

In accordance with AFI 10-712, *Telecommunications Monitoring Assessment Program*, I have determined 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.

LAWYER B. JUSTICE, Col, USAF
Judge Advocate

2nd Ind, MAJCOM, DRU, FOA JA xx May xx

TO: 123d CS

In accordance with AFI 10-712, *Telecommunications Monitoring Assessment Program*, I have determined 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.

JUSTICE LAWYER, Col, USAF
Judge Advocate

Attachment 6

NOTICE AND CONSENT CHECKLIST

Figure A6.1. Notice And Consent Checklist

MANDATORY ACTIONS CHECK ALL ITEMS FOR COMPLIANCE	YES	NO
Base/Installation Telephone Directories: **Does the base telephone directory contain the Notice and Consent statement from AFI 10-712, Paragraph 4.2** Statement must be prominently displayed on the front cover of hard copy telephone directory. If the telephone directory is embedded in a base information guide, the statement must appear on the first page of the official portion of the telephone directory. Statement must be at the top of the first page of electronic versions. Provide a copy of the telephone directory cover, first page of the telephone directory portion of a base guide and/or the first page of the electronic phone directory.	_____	_____
Telephones: **Do all telephones (including STEs) have a DD Form 2056 or similar sticker affixed on the front?** If using a locally created consent sticker, ensure the Notice and Consent verbiage is identical to the DD Form 2056. Provide a copy of any locally generated Notice and Consent stickers.	_____	_____
Facsimile Machines (FAX): **Do all facsimile machines have a DD Form 2056 or a locally created sticker attached?** If using a locally created sticker, ensure the Notice and Consent verbiage is identical to the DD Form 2056. Provide a copy of any locally generated Notice and Consent stickers. **------AND----** **Is AF Form 3535 facsimile cover sheet, or locally generated fax cover sheet, used for all fax transmissions?** If using a locally generated fax cover sheet, ensure the Notice and Consent statement is identical to statement shown at AFI 10-712, Paragraph 4.4.2. Provide a copy of any locally generated fax cover sheets.	_____ _____	_____ _____

<u>Portable Electronic Devices (cellular phones, text pagers, PDAs, LMRs etc)</u>: **Do all users of Portable Electronic Devices (PED) sign a user agreement with the exact Notice and Consent statement from AFI 10-712, Paragraph 4.7.1.?** Provide a copy of the agreement with the Notice and Consent statement. **Do all LMRs issued without a signed user agreement have the DD Form 2056, Telephone Monitoring Notification Decal, Affixed?**	_____ _____	_____ _____
<u>Information System Notice and Consent Banner:</u> **Do all Information Systems display the required current log-in banner in full view or requires the user to scroll the through the entire banner before requiring user acknowledgement to proceed?** **If system limitations exist, has the abbreviated banner been installed?** If there are extenuating circumstances or cost prohibitions, has the MAJCOM or DRU /A6 been contacted to determine their choice of appropriate action from the options given in AFI 10-712, Para 4.5.2.?	_____ _____	_____ _____
<u>Private/Intranet Web Sites and Homepages</u>: **Does the first page on all unit private/intranet web sites and homepages have the current Notice & Consent banner prominently displayed?** NOTE: Public Web Sites/Pages - Notice and Consent requirements (AFI 10-712 do not apply to public web sites/pages. See AFI 10-712 paragraph 4.6, for Privacy and Security Notice requirements for public web sites/pages.		
<u>Telecommunications devices</u>: **Do all telecommunications devices not otherwise referenced in AFI 10-712 have users signed receipt with following statement?** **"This telecommunications device is subject to monitoring at all times. Using this device constitutes consent to monitoring."**	_____	_____
Are all supported DRUs, FOAs, GSUs, and Tenants listed by name in the package (paragraph 1 of summary letter)?	_____	_____
<u>INSTALLATION JA:</u> **Does the package contain sufficient detailed information to conduct a legal review to determine compliance with AFI requirements for notifying users of telecommunications systems that their use constitutes consent to monitoring?**		

Do the measures and actions taken by the base demonstrate, in the aggregate, that all users of telecommunications systems are on notice that their communications may be monitored? **Does your endorsement support the rationale that the measures and actions taken by the base demonstrated that all users of telecommunications systems have been given proper notice of and consented to their communications being monitored?** The package contains the following required attachments: 1) Telephone Directory Cover ____ 2) Print Screen of Electronic Telephone Directory Web Page ____ 3) Copy locally produced FAX cover sheet, if used ____ 4) Copy of PED user agreement(s)____ 5) Print Screen of Computer Banner ____ **6)** Print Screen of Unit Private Web Pages with Banner ____	_____ _____ _____	_____ _____ _____
<u>MAJCOM, DRU, FOA JA:</u> **Were concerns addressed by the base JA corrected before the package was forwarded and does the package include the base JA's endorsement?** MAJCOM, DRU, FOA JA POC NAME:_____ Signature:_____ Date:_____	_____	_____
<u>INSTALLATION IA OFFICE:</u> **Does the package meet IA Notice and Consent requirements and is a separate Installation JA and MAJCOM, DRU, FOA JA endorsement included?** INSTALLATION IA POC NAME:_____ Signature:_____ Date:_____	_____	_____