

**BY ORDER OF THE SECRETARY  
OF THE AIRFORCE**

**AIR FORCE INSTRUCTION 10-712**

**17 DECEMBER 2015**



**Operations**

**CYBERSPACE DEFENSE ANALYSIS  
(CDA) OPERATIONS AND NOTICE  
AND CONSENT PROCESS**

**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](http://www.e-Publishing.af.mil)

**RELEASABILITY:** There are no releasability restrictions on this publication

---

OPR: AF/A3OY

Certified by: HQ USAF/A35  
(Maj Gen Martin Whelan)

Supersedes: AFI10-712, 8 June 2011

Pages: 47

---

This publication 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 provides responsibilities, procedures, and guidance for the Air Force's Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process. It conforms to national and Department of Defense (DOD) directives pertaining to the monitoring of unsecure electronic communication for information content. It applies to individuals at all levels including the Air Force Reserve and Air National Guard (ANG), except where otherwise noted, who use Air Force controlled DOD electronic communication 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. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, or T-3) number following the compliance statement. See AFI 33-360, Publications and Forms Management, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. This publication may be supplemented at any level, but all supplements must be routed to the Office of Primary Responsibility (OPR) listed above for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the

field through the appropriate chain of command. Requests for waivers must be submitted to the OPR listed above, or as otherwise stipulated within this publication, for consideration and approval. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

### ***SUMMARY OF CHANGES***

The publication has been revised. This rewrite of AFI 10-712 includes the introduction of the CDA weapon system (WS) with its three mission sets; the title change from Telecommunication Monitoring Assessment Program (TMAP) to CDA Operations and Notice and Consent Process; and identifies tiered waiver authorities for unit level compliance items IAW AFI 33-360, *Publications and Forms Management*. Changes to this document include the roles for MAJCOM, DRU, and FOA Operations Security (OPSEC) Program Managers (PM), expanded explanation of the CDA WS products and procedures, updates to the notice and consent procedures and timelines.

<b>Chapter 1— GENERAL</b>	<b>4</b>
1.1. Overview.....	4
1.2. Purpose.....	4
1.3. CDA Authority. ....	4
Figure 1.1. Cyberspace Defense Analysis Mission Breakdown.....	6
1.4. Notice and Consent. ....	7
1.5. Roles and Responsibilities. ....	8
<b>Chapter 2— DISTRIBUTION OF ESSA PRODUCTS</b>	<b>18</b>
2.1. Focused Look Assessment Request Procedures. ....	18
Figure 2.1. CDA Mission Request Process Flow .....	19
2.2. Distribution of ESSA Products. ....	19
2.3. ESSA Products.....	20
2.4. Types of ESSA Products.....	20
<b>Chapter 3— ESSA ATTRIBUTION AND UNIQUE REPORTING</b>	<b>23</b>
3.1. Release of ESSA Information. ....	23

<b>AFI10-712 17 DECEMBER 2015</b>	<b>3</b>
3.2. Use and Control of ESSA Products; Situational Guidance.....	23
3.3. Assessment Preparation. ....	25
3.4. Team Travel and Funding. ....	25
3.5. Quality Control (QC). ....	26
<b>Chapter 4— NOTICE AND CONSENT PROCEDURES</b>	<b>27</b>
4.1. Notification. ....	27
4.2. Telephone Directories. ....	27
4.3. Telephones. ....	27
4.4. Facsimile Machines and Multi-Function Devices. ....	27
4.5. Information Systems. ....	28
4.6. Private or Intranet Web Home pages. ....	28
4.7. Portable Electronic Devices (PED).....	28
4.8. Other Information Technology. ....	29
4.9. Optional Notice and Consent Awareness Methods.....	29
4.10. Notice and Consent Certification Process.....	29
4.11. Notice and Consent Certification Schedule. ....	32
Table 4.1. Notice and Consent Certification Schedule .....	32
<b>Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>34</b>
<b>Attachment 2— STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER</b>	<b>39</b>
<b>Attachment 3— MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS</b>	<b>40</b>
<b>Attachment 4— NOTICE AND CONSENT MEMORANDUM WITH 1ST AND 2ND IND</b>	<b>42</b>
<b>Attachment 5— NOTICE AND CONSENT CHECKLIST</b>	<b>45</b>

## Chapter 1

### GENERAL

**1.1. Overview.** The Air Force (AF) uses electronic communications systems such as telephones, cellular phones, radios, pagers, computers, 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. Electronic System Security Assessment (ESSA) provides commanders with an assessment as to the type and amount of information traversing Department of Defense (DOD) electronic communication systems that is at risk to adversary collection and exploitation. ESSA products can be used to evaluate personnel compliance with Information, Personnel, and Industrial Security practices; Communications Security (COMSEC) and Cybersecurity procedures, and the implementation of Military Deception, and Operations Security (OPSEC) activities. ESSA products are also used to support other security operations, activities, and programs to enhance force protection, and focus training requirements.

**1.2. Purpose.** The Air Force conducts ESSAs using the CDA WS to support OPSEC analysis of protection measures for AF Core Functions. ESSA monitoring involves the collection and analysis of information transmitted via DOD electronic communication systems. These systems can include radios, wired or wireless telephones, and computer networks. ESSA products help commanders evaluate their organization's Information, Personnel and Industrial Security practices; COMSEC, Wing Cybersecurity office, and OPSEC posture by determining the amount and type of information available to adversary collection entities.

1.2.1. The AF monitors, collects, and analyzes information from DOD electronic communications systems to determine if any critical or classified information transmitted via unsecured and unprotected systems could adversely affect US (and allied/coalition) operations.

1.2.2. CDA operations are an integral part of AF OPSEC, Information Operations (IO), and Red Teaming. 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, technical, and physical security procedures routinely surface as possible sources of intelligence losses.

**1.3. CDA Authority.** Headquarters Air Force Space Command (HQ AFSPC) CDA elements (including its gained or associated reserve units) are the only AF organizations authorized to conduct CDA activities. These activities are accomplished within certain legal parameters utilizing authorized tools to monitor, collect, and transfer telecommunication data for analysis. They perform CDA activities in a manner that satisfies the legitimate needs of the AF to provide OPSEC assessments while protecting the legal rights and civil liberties of those persons whose communications are subject to CDA monitoring.

1.3.1. The authority to monitor AF networks in the course of network defense is derived from the service provider exceptions to the *Electronic Communications Privacy Act*, 18 USC 2111(2)(a)(i) and 18 USC 3121(b)(1); the 2008 National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), which directed

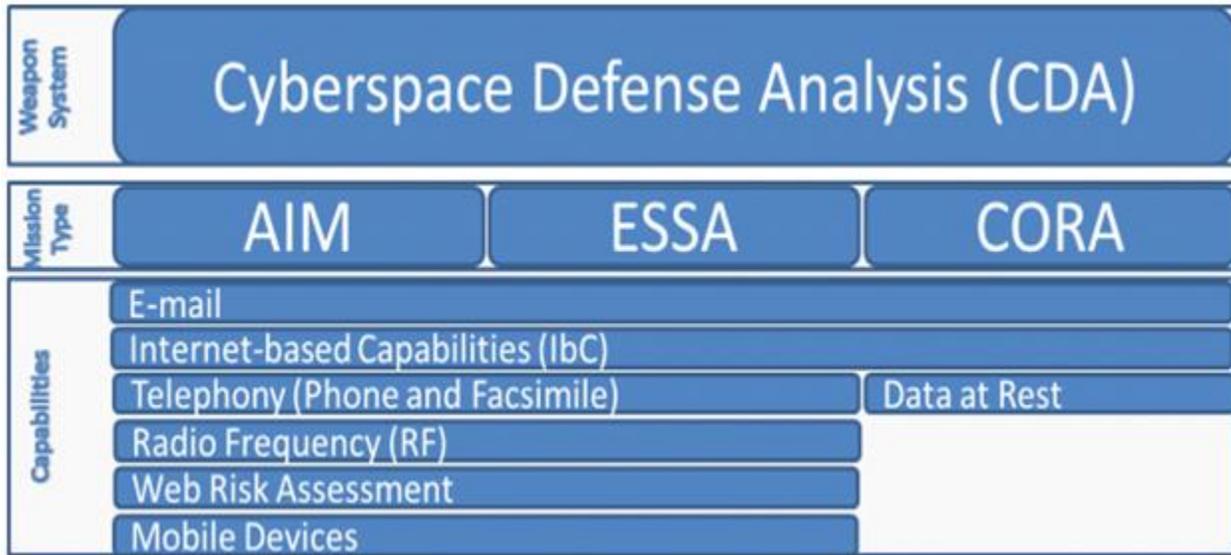
initiatives to monitor Federal information systems for network security purposes; the National Defense Authorization Act (NDAA) Section 931, codified as a note to 10 USC 2223, NDAA 2012, Section 953; Department of Defense Directive (DODD) O-8530.1, *Computer Network Defense*, and DOD Instruction (DODI) 8500.01, *Cybersecurity*.

1.3.2. CDA Missions: The CDA WS currently conducts three separate missions: Active Indicator Monitoring (AIM) in support of cyberspace network defense and ESSA in support of OPSEC mission sets and Cyberspace Operations Risk Assessment (CORA) in support of Cybersecurity.

1.3.2.1. AIM – Protect the Air Force, DOD and government networks. AIM missions identify and report disclosed information that could be used to gain authorized access to compromise Air Force Networks and devices. AIM tools include, but are not limited to e-mail and IbC.

1.3.2.2. ESSA- Protect information pertaining to Air Force, DOD and government operations, capabilities, and resources. ESSA missions identify and report disclosed information that could be used to compromise missions, gain access to sensitive capabilities, and deny knowledge of critical resources. ESSA utilizes the following tools: telephony, e-mail, IbC, radio frequency (RF), and web risk assessment (WRA). Authority is derived from DODI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*.

1.3.2.3. CORA - Mitigate the effects of lost Air Force, DOD and government operations, capabilities, and resources. CORA missions analyze potential and confirmed compromised data from adversary exfiltration or friendly transmission outside of U.S. Government control, with the objective of determining the associated impact to Air Force operations and technology resulting from the data loss. CORA applies OPSEC principles and processes in the conduct of responsive and systematic analysis of the content of compromised data leaving the AFIN. While there are other similar capabilities analyzing compromised computers and networks, they are focused on methods, techniques, system vulnerability identification, and the identification or attribution of an adversary. CORA is a contributor to the overall Information Damage Assessment (IDA) process based on evidence that data was or potentially exfiltrated from an AF system due to adversaries' cyber activities. When conducting CORA missions CDA units are not monitoring or collecting any information from the AFIN. CORA is focused on the nature and content of the compromised information itself, and the potential impact of its loss within the final IDA product. CORA capabilities assist information owners in determining the operational risk and impact of compromised information. CORA utilizes the following tools: e-mail, IbC and Data at Rest. Authority is derived from AFI 10-1701, *Command and Control (C2) for Cyberspace Operations*.

**Figure 1.1. Cyberspace Defense Analysis Mission Breakdown.**

1.3.3. The AF conducts continuous monitoring that can be tasked and focused to defend specific information via Information Defense Priorities. Information Defense Priorities can be based on Air Force organizations, mission sets, capabilities, weapon systems, platforms, or any other significant categorization of Air Force owned information.

1.3.3.1. All organization OPSEC Program Managers (OPSEC PM) will supply CDA units with Information Defense Priorities through their major command (MAJCOM) or direct reporting unit (DRU) OPSEC PM for inclusion in the continuous monitoring mission. (T-1).

1.3.3.2. OPSEC PMs and members of the AF OPSEC Support Team (AF OST) can request a Focused Look Assessment through their MAJCOM, DRU, or field operating agency (FOA) OPSEC PM that includes any number of Information Defense Priorities specific to a single Air Force core function, organization, mission set, capability, or weapon system. A Focused Look Assessment can cover multiple organizations, installations, or locations.

1.3.3.3. Organization requested Focused Look Assessments are submitted by the Headquarters AF (HAF), AF OST, MAJCOM, DRU, or FOA OPSEC PM to the 624th Operations Center (OC). Most CDA activities are provided at no cost to the assessed organization. However, if the assessed organization's requires a mode of monitoring (e.g., RF, ref para. 1.3.4.4 and 3.5.) requiring physical proximity or requests an in-person mission out-brief, the requesting organization must fund the travel of the CDA team performing the ESSA mission. Refer to paragraph 3.1 for further details. Monitoring resources can 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 intelligence collection and exploitation. These assessments are also conducted to provide information and data into the OPSEC risk analysis process, gauge the overall effectiveness of a program or operation, and to support cybersecurity objectives.

1.3.4. The following ESSA monitoring capabilities are available to a commander and the AF OST:

1.3.4.1. Telephony – The monitoring and assessment of AF unclassified voice networks which if exploited by adversaries, can negatively impact AF operations.

1.3.4.2. Email Communications – The monitoring and assessment of unclassified AF email traffic entering or exiting the AFIN which if exploited by adversaries, can negatively impact AF operations.

1.3.4.3. IbC – The monitoring and assessment of unencrypted SMTP and HTTP communications that either enter or leave the AF Gateway architecture. **NOTE:** CDA units only “monitor” the web sessions that transverse the AFIN 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.).

1.3.4.4. Radio Frequency (RF) Communications – The monitoring and assessment of AF communications within the VHF, UHF, FM, HF, and SHF frequency bands (e.g., mobile phones, land mobile radios, wireless local area networks) which if exploited by adversaries, can negatively impact AF operations.

1.3.4.5. Cyber Operations Risk Assessment (CORA) –The analysis of compromised data from adversary exfiltration or friendly transmission outside of U.S. Government control, with the objective of determining the associated impact to Air Force operations and technology resulting from the data loss. CORA applies OPSEC principles and processes in the conduct of responsive and systematic analysis of the content of compromised data leaving the AFIN. While there are other similar capabilities analyzing compromised computers and networks, they are focused on methods, techniques, system vulnerability identification, and the identification or attribution of an adversary. CORA is a contributor to the overall IDA process. It is focused on the nature and content of the compromised information itself, and the potential impact of its loss within the final IDA product. CORA capabilities assist information owners in determining the operational risk and impact of compromised information.

1.3.4.5.1. CORA is a specific assessment that can be generated by user request, as a 624 OC directed follow-on tasking after compromised data is discovered or as a near real-time assessment to support mission assurance or information damage assessment.

1.3.4.5.2. Reports generated as a result of a CORA tasking are not subject to the limiting instructions of other ESSA reports. CORA reports may be used for subsequent reports, such as Foreign Intelligence or Counterintelligence bulletins.

1.3.4.6. WRA – The 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.

**1.4. Notice and Consent.** Although not a part of the CDA WS, notice and consent is a legal requirement before monitoring can be conducted, and is therefore integrated into this instruction. All authorized users of communications systems and devices must receive notice that monitoring is conducted and use of the system or device constitutes consent to monitoring. All DOD

electronic communication 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*.

1.4.1. Objectives. The processes outlined in this publication ensure compliance with legal requirements associated with notifying personnel of electronic communication monitoring and their consent by using these devices. They also do the following:

1.4.1.1. Provide implementation guidance for the exact content of a warning banner as specified by current DOD direction (see Attachments 3 of this instruction for reference).

1.4.1.2. Establish a primary reference and additional implementation guidelines for Cybersecurity Control ECWM-1, Warning Message, according to the requirements of DODI 8500.01, *Cybersecurity*.

1.4.1.3. Establish guidance and provide procedures for accomplishment of the biennial Cybersecurity Notice and Consent Certification according to DODI 8560.01.

1.4.1.4. CDA units will ensure a current notice and consent certification has been approved by SAF/GC prior to conducting operations. **(T-0)**.

1.4.1.5. Chapter 4 provides complete details on notice and consent certification procedures.

## **1.5. Roles and Responsibilities.**

1.5.1. **Joint Communications Security (COMSEC) Monitoring Activity (JCMA)**. JCMA conducts communications monitoring across the DOD. JCMA can request Air Force support for its tasked missions through 624 OC. JCMA requests should be levied as a joint requirement and executed under the Joint Operations Planning and Execution System.

1.5.2. **The Department of Defense Chief Information Officer (DOD CIO)**. Has sole approval authority for communications security (COMSEC) monitoring and cybersecurity 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.

1.5.3. **The Secretary of the Air Force (SECAF)**. Approves COMSEC monitoring and cybersecurity readiness testing of AF owned or leased systems IAW DODI 8560.01. This authority may be delegated.

1.5.4. **The Office of the Secretary of the Air Force General Counsel (SAF/GC)**.

1.5.4.1. Provides oversight and guidance on all legal matters pertaining to CDA WS procedures and activities.

1.5.4.2. Reviews and provides consultation regarding the use of CDA WS derived information in disciplinary proceedings including courts-martial, non-judicial punishment, and adverse administrative proceedings.

1.5.4.3. Biennially, during even-numbered years, reviews reports forwarded by each AF installation, and certifies those installations that meet notice and consent requirements as eligible for monitoring.

**1.5.5. The Administrative Assistant to the Secretary of the Air Force (SAF/AA).** Provides coordination and integration of CDA WS policy and guidance through the Air Force Security Enterprise Executive Board.

**1.5.6. The Secretary of the Air Force, Office of Public Affairs (SAF/PA).** Develops policy and guidance on the process for releasing information to the public. Also, ensures public web sites receive initial security and policy review prior to site launch.

**1.5.7. The Secretary of the Air Force Information Dominance and Chief Information Officer (SAF/CIO A6).** Proposes policy for notice and consent certification and related matters.

**1.5.8. The Deputy Chief of Staff for Operations (AF/A3).** The Director of Future Operations (AF/A35) is the office of primary responsibility (OPR) for establishing policy and guidance for the CDA WS.

1.5.8.1. Provides oversight, advocacy, and acts as a focal point for the AF CDA WS.

1.5.8.2. Develops AF Departmental publications to define policy, guidance, responsibilities, and authorities to establish the internal management processes necessary to carry out DOD policy/guidance.

1.5.8.3. Ensures those performing CDA Operations 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.

1.5.8.4. Advocates for program funding for CDA through established budgeting and requirements processes.

1.5.8.5. Coordinates assessment procedures with joint staff, National Security Agency (NSA), and other DOD components when joint systems carry AF communications of interest.

**1.5.9. Headquarters Air Force Space Command, Directorate of Integrated Air, Space, Cyberspace, and ISR Operations (HQ AFSPC/A2/3/6)** organizes, trains, and equips forces for the CDA WS and Notice and Consent. Additionally:

1.5.9.1. Organizes, trains, and equips forces to provide combatant commanders with communication monitoring capabilities.

1.5.9.2. Ensures the implementation of AF communication monitoring requirements established within this instruction.

1.5.9.3. Provides CDA resources to assist AF organizations in assessing their electronic communications.

1.5.9.4. Ensures CDA focuses on the collection and analysis of information transmitted via unsecured DOD electronic communications systems and information secured but stored on unencrypted and uncontrolled systems.

- 1.5.9.5. Coordinates with AF/A35 on all current and future AF CDA WS requirements, processes, and resources.
- 1.5.9.6. Coordinates assessment capabilities with the Joint Staff, National Security Agency (NSA), and other DOD Components to standardize equipment/processes and increase interoperability.
- 1.5.9.7. Generates new ideas and concepts to continuously improve the AF CDA WS.
- 1.5.9.8. Integrates CORA capabilities into the overall AF Information Damage Assessment process.
- 1.5.9.9. Considers the integration and use of ESSA and/or ESSA products with other security support capabilities, efforts, or initiatives.
- 1.5.9.10. Authorizes ESSA procedures.
- 1.5.9.11. Performs periodic annual security assessments to ensure CDA tools continue to minimize the risk of critical, sensitive, or classified data proliferation outside of the CDA secure network enclave environment.
- 1.5.9.12. Review quality control evaluation reports during staff assistance visits and through the Inspector General process to ensure compliance with the appropriate instructions and pamphlets. CDA units will establish procedures for an aggressive QC program. **(T-1)**. At a minimum, procedures will contain a sample evaluation of individual product and trends analysis reporting at least semiannually. **(T-1)**. Documentation records of evaluations are maintained and trend reports are coordinated with formal training programs to enhance the training process. (See Section 3.5 of this instruction.)
- 1.5.9.13. Submits recommendations for development of policy and guidance regarding AF Notice and Consent to AF/A35.
- 1.5.9.14. Reviews, interprets, and evaluates national and DOD Notice and Consent guidance, and make recommendations on implementation to SAF/CIO A6 and SAF/GCI.
- 1.5.9.15. Biennially, during even-numbered fiscal years:
- 1.5.9.15.1. Coordinates with MAJCOM, DRU, FOA, and Wing Cybersecurity offices to prepare for biennial reporting procedures.
  - 1.5.9.15.2. Acts as the focal point for the notice and consent certification process.
  - 1.5.9.15.3. Maintains copies of installation notice and consent memorandums (see Attachment 4 of this instruction) for all installations until SAF/GC has authorized initiation or continuation of monitoring at all Air Force installations.
  - 1.5.9.15.4. Provides certification cycle guidance and support to MAJCOM, DRU, FOA, and Wing Cybersecurity offices.
  - 1.5.9.15.5. Works with MAJCOM and DRU A6 offices to ensure subordinate installations adhere to established procedures and timelines within this guidance.
  - 1.5.9.15.6. Submits all finalized Notice and Consent Summary Reports with endorsements to SAF/GC with courtesy copy to HQ AFSPC/A3 and 24 AF.

- 1.5.9.15.7. Reviews report received from each AF installation, ensuring accurate and acceptable reporting of mandatory notice and consent actions over the previous 24 months.
- 1.5.9.15.8. Coordinates required corrective actions identified through the review process with the relevant Wing Cybersecurity Office including their respective MAJCOM/A6 in all correspondence.
- 1.5.10. Headquarters Air Force Space Command, Requirements (HQ AFSPC/A5):**
- 1.5.10.1. Develops requirement documentation and (as required) funding documents in coordination with HQ AFSPC/A3 to procure improved capabilities and ensure maintenance of the AF CDA WS.
- 1.5.10.2. Complies with appropriate AF acquisition, evaluation, and contracting processes.
- 1.5.10.3. Develops and maintains operational capability requirement documents for conducting all CDA operations.
- 1.5.11. Major Command (MAJCOM), Direct Reporting Unit (DRU), and Field Operating Agency (FOA)/A6:**
- 1.5.11.1. Ensures all subordinate units are identified for inclusion in the SAF/GC Certification letter.
- 1.5.11.2. Assists AFSPC A2/3/6 with Notice and Consent process as per guidance in paragraph 4.10.5 of this instruction.
- 1.5.12. MAJCOM, DRU, and FOA Information Protection Offices:**
- 1.5.12.1. Route classification mission data determinations to the appropriate MAJCOM, DRU, or FOA original classification authority and subject matter expert (SME).
- 1.5.12.2. Initiate security incidents as required, in accordance with AFI 31-401, Information Security Program Management.
- 1.5.12.3. Monitor original classification authority damage assessments for any classified information that has been compromised.
- 1.5.13. MAJCOM, DRU, and FOA PM:**
- 1.5.13.1. Manage their command's request for CDA support through directing, soliciting, prioritizing, and consolidating assessment requests. **(T-1)**.
- 1.5.13.2. At a minimum, each MAJCOM and DRU will request two Focused Look Assessments, per fiscal year. **(T-1)**.
- 1.5.13.3. At a minimum, each FOA will request one Focused Look Assessment, per fiscal year. **(T-1)**.
- 1.5.13.4. Prior to submitting a Focused Look Assessment request to the 624 OC, DRUs and FOAs should coordinate the request with the host installations OPSEC PMs to avoid conflicts with other operations. **(T-1)**. If a host installation is requesting a Focused Look Assessment, the DRUs and/FOAs should consider consolidating their request.

1.5.13.5. Act as the focal point for all CDA products as listed in paragraph 2.2 of this instruction at the organization level. (T-1).

1.5.13.6. Forward CDA products to the affected subordinate organization with a requirement to provide feedback concerning the mediation of the vulnerability back to the higher headquarters (HHQ) OPSEC PM to ensure closure of all ESSA vulnerability findings. (T-1).

1.5.13.7. In the organization's Annual OPSEC Program Report, account for the number of Focused Look Assessment support requests submitted, support request fulfilled, and the affect results had on the organization's mission. (T-1).

1.5.13.8. Provide feedback to CDA units concerning assessments conducted and actions taken as a result of disclosures and trends. (T-1).

1.5.13.9. Provide pre-mission information to AF CDA units two weeks prior to mission start when possible to allow for pre-mission setup. (T-1).

1.5.14. **MAJCOM, DRU, and FOA/JA:** Reviews and endorses installation notice and consent biennial packages as per guidance in paragraph 4.10.6 of this instruction.

1.5.15. **National Air and Space Intelligence Center (NASIC)** provides requested threat data to the 624 OC for further distribution. This is currently delegated to NASIC OL-A.

1.5.16. **24th Air Force (24 AF):**

1.5.16.1. Directs all worldwide CDA missions.

1.5.16.2. Approves all CDA missions for execution (can be delegated).

1.5.16.3. Ensures CDA lessons learned and best practices are submitted to the AF Lessons Learned Joint Lessons Learned Information System (JLLIS).

1.5.16.4. Maintains oversight of standardization and evaluation program for CDA operations.

1.5.16.5. Deploys CDA forces as the sole Air Force CDA force provider for contingencies.

1.5.16.6. Establishes standardization and evaluation processes for CDA operations.

1.5.16.7. Authorizes the execution of CDA missions without prior notification on any AF unclassified telecommunication system certified by SAF/GC for consent to monitor.

1.5.16.8. Performs CDA activities only at installations where notice and consent procedures are certified as legally sufficient by SAF/GC as stated in **Chapter 4**, Attachment 4 of this instruction.

1.5.16.9. Ensures all AF Core Functions are assessed at least once per year and results from these assessments are provided to the affected Command OPSEC PM and the Command OPSEC PM of the AF Core Function Lead Integrators. These assessments can include telephone, e-mail, IbC, and WRA mission subsets.

1.5.16.10. Ensures CDA support is provided to the AF OST for AF focused OPSEC External Assessments.

**1.5.17. The 624th Operations Center (624 OC):**

1.5.17.1. Tasks CDA WS resources to support requests for CDA missions. The 624 OC weighs competing objectives when prioritizing requests, maximizes the employment of CDA resources, and balancing workloads.

1.5.17.2. Schedules CDA activities only for electronic communications to and from installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

1.5.17.3. Schedules wireless communications monitoring only when the monitoring equipment is technically capable of isolating monitoring to specific AF telecommunication devices. If the equipment utilized cannot demonstrate clearly and specifically this capability, seek a legal review from 67<sup>th</sup> Cyberspace Wing (CW)/JA before tasking the assessment.

1.5.17.4. Establish and maintain on SIPRNET an automated repository of AIM and ESSA reports, CDA Support request forms and templates accessible to all AF MAJCOM, DRU, and FOA OPSEC PMs to mitigate discovered vulnerabilities, aid in the development of future CDA capability reports, and OPSEC awareness efforts.

**1.5.18. 67 CW:**

1.5.18.1. Responsible for full spectrum network and cyberspace operations for the AF, including CDA operations.

1.5.18.2. Can submit nominations for Information Defense Priorities or Focused Look Assessments to the 624 OC for inclusion in future tasking's.

1.5.18.3. Can submit recommended prioritization of CDA tasking to the 624 OC.

1.5.18.4. In coordination with 24 AF/JA, develops and implements procedures to protect the legal rights and civil liberties of persons whose communications are subject to assessment.

1.5.18.5. Executes tasked missions through subordinate organizations.

1.5.18.6. Executes the standardization and evaluation program.

1.5.18.7. Coordinates with and submits CDA operations resource requirements to HHQ for evaluation and inclusion in AF Program Objective Memorandum process (POM).

1.5.18.8. Ensures CDA units establish data retention, archival and back-up policies and procedures IAW AFMAN 33-363, *Management of Records and AF Records Disposition Schedule in the Air Force Records Information Management System (AFRIMS)*. Adoption or modification of existing database management best practices will meet this requirement. **(T-1)**. Destroy non-operational data as soon as operationally feasible, but no later than 90 days from the collection date. Retain all other mission related data (reports, transcripts, trip reports, site surveys, etc., and any associated collected data) for 2 years after fiscal year in which created or they are obsolete whichever is sooner. No unsorted collected data will be kept for longer than 90 days. **(T-3)**. EXCEPTIONS: Maintain data as required to support compliance with Federal laws and supporting AFIs that supersede this instruction. Any data supporting training requirements can be

indefinitely retained. Personally identifiable information (PII) data should only be retained for formal training purposes.

1.5.18.9. Ensure CDA units develop a process to rapidly report situations when an IbC and/or data monitoring vulnerability assessment reveal information which requires immediate action.

1.5.18.10. The 67 CW/JA provides legal reviews of any proposed use or development of ESSA derived information in disciplinary proceedings including courts-martial, non-judicial punishment, and adverse administrative proceedings. The 67 CW/JA will note any conflicts with Federal laws or Congressional mandates to 24AF/JA and HQ AFSPC/JA. **(T-1)**. SAF/GCI will consult on the proposed use of ESSA derived evidence in legal actions to include courts-martial, non-judicial punishment, and adverse administrative proceedings. **(T-1)**.

1.5.18.11. Collects and analyzes all CDA products developed by authorized CDA units (including gained or associated reserve units), identifies trends as described in 1.5.9.13 of this instruction.

#### 1.5.19. **CDA units:**

1.5.19.1. Comply with this instruction and HHQ policies/guidance.

1.5.19.2. Perform CDA activities only for electronic communications to and from installations where notice and consent procedures are certified as legally sufficient by SAF/GC.

1.5.19.3. Monitor and assess AF electronic communication to satisfy legitimate information protection requirements.

1.5.19.4. Identify and evaluate the content of AF public and private web site data including text based, image, audio, and video. (May not be applicable to all CDA units.)

1.5.19.5. Ensure monitoring requests are forwarded to the 624 OC for action.

1.5.19.6. Conduct CDA activities only on AF owned or leased electronic communication systems or devices, except for JCMA tasked support IAW paragraph 1.5.1 of this instruction.

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

1.5.19.8. Will not use tone-warning devices when using recording equipment for ESSAs. **(T-0)**.

1.5.19.9. Will not retain PII or sensitive PII after reporting as prescribed in paragraph 3.2 and 3.2.6. Promptly destroy any such information collected as directed by paragraph 1.5.18.8 of this instruction. **(T-0)**.

1.5.19.10. Will report immediately IAW paragraph 3.2 of this instruction:

1.5.19.10.1. Any emergency situation threatening death, serious bodily harm or major loss of property. **(T-0)**.

- 1.5.19.10.2. Any indication of a potential or ongoing serious criminal or counterintelligence concern. **(T-0)**.
- 1.5.19.11. Identifies non-material solutions to tactical deficiencies by submitting a Tactics Improvement Proposal IAW AFI 11-260, *Tactics Development Program*, to HHQ.
- 1.5.20. Wing and Installation Commanders/Directors:**
- 1.5.20.1. Send assessment requests to their respective MAJCOM, DRU, or FOA OPSEC PM. **(T-1)**.
- 1.5.20.2. Consider using CDA support in appropriate operations and exercise plans.
- 1.5.20.3. Comply with paragraph 3.2.9 prior to taking UCMJ action including non-judicial punishment actions based on CDA products. **(T-1)**.
- 1.5.20.4. Ensures the OPSEC PM is appointed as the OPR to coordinate the activities of CDA units when scheduled to receive an assessment. **(T-1)**. The OPSEC PM or OPSEC PMs:
- 1.5.20.4.1. As required, coordinate with the appropriate network control officials and/or information protection offices to facilitate the remediation and containment of any classified information identified during the operation.
- 1.5.20.4.2. Coordinate the needs of the CDA team and assists with assessment preparation. Typical actions for this responsibility are available in Chapter 3.
- 1.5.21. The Installation Legal Offices (JA):**
- 1.5.21.1. Review and endorse installation notice and consent biennial packages, validating compliance with applicable laws and paragraph 4.10.4 of this instruction. **(T-1)**.
- 1.5.21.2. Contact 67 CW/JA regarding use of CDA developed information as evidence prior to advising commanders on any potential punitive, disciplinary or adverse personnel action when the advice relies on such evidence. **(T-1)**.
- 1.5.21.3. For Joint installations, review local service agreements for thorough coverage of Notice and Consent responsibilities and compliance with this instruction and DODI 8560.01. **(T-1)**.
- 1.5.22. Wing Cybersecurity Offices** Ensures compliance with Notice and Consent requirements when performing annual cybersecurity assessments per AFI 33-230, *Information Assurance Assessment and Assistance Program* and will:
- 1.5.22.1. Generate and submit a Notice and Consent summary package biennially according to Chapter 4 of this instruction. **(T-0)**.
- 1.5.22.2. Obtain and provide any Unit/JA, MAJCOM/JA, HQ AFSPC/A2/3/6, JA, or SAF/GCI requested corrections or clarifications. **(T-1)**.
- 1.5.22.3. Maintain a copy of the installation's finalized notice and consent summary report and SAF/GC Notice and Consent Authorization Memo until the end of the next biennial certification cycle. **(T-3)**.

1.5.22.4. For joint installations, ensure sufficient local service agreements are in-place to provide thorough coverage of Notice and Consent responsibilities and compliance with this instruction and DODI 8560.01. **(T-2)**.

1.5.22.5. Notify HQ AFSPC/A2/3/6 of any organizational changes affecting the next Notice and Consent certification cycle. **(T-2)**.

**1.5.23. Organizational Cybersecurity Offices** are responsible for management and execution of the Notice and Consent Program IAW AFMAN 33-282, *Computer Security (COMPUSEC)*, and will:

1.5.23.1. Perform annual self-assessments of all information technology to ensure compliance with this guidance using the Management Internal Control Toolset (MICT) and Chapter 4 of this instruction. **(T-1)**.

1.5.23.2. Document deficiencies found during the assessments in the organizational cybersecurity detailed report and the COMPUSEC Self-Assessment Communicator (SAC) A6-2-2 within the MICT. **(T-1)**.

1.5.23.3. Correct deficiencies identified within 30 days of the cybersecurity assessment. **(T-3)**.

1.5.23.4. Document and track corrective actions within their cybersecurity program to ensure reporting of compliance on the biennial report. **(T-2)**.

1.5.23.5. Ensure the first pages on all the organizations private/intranet web home pages comply with paragraph 4.6 of this instruction. **(T-1)**.

1.5.23.6. Submit a biennial report to the Wing Cybersecurity office (see Attachment 5 of this instruction). **(T-1)**.

1.5.23.7. 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 AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, and by implementing the notices in Chapter 4. **(T-1)**.

1.5.23.8. Ensure that each individual issued a portable electronic device (PED) signs an AF Form 4433, IAW AFMAN 33-282, *Computer Security, (COMPUSEC)*.

1.5.23.9. Ensure individuals issued a Land Mobile Radio (LMR) sign an AF Form 4433 unless a DD Form 2056 is attached to the device.

1.5.23.10. Apply paragraph 3.2.4 of this instruction if classified information is found during the course of a CDA mission. **(T-1)**.

1.5.23.11. Ensure organizations to include GSUs have received a current notice and consent certification. **(T-1)**.

**1.5.24. Training Program Managers.** Upon request, CDA units can release any ESSA derived mission data subject to the requirements of paragraph 1.5.14.8, of this instruction, to support training programs. Trainers and instructors will:

1.5.24.1. Control access to the recorded communications. **(T-1)**.

1.5.24.2. Label the recorded electronic communications as containing information obtained through communications monitoring. **(T-3)**.

1.5.24.3. Inform all students and instructors, in writing that recorded communications are only for classroom discussion. **(T-3)**.

## Chapter 2

### DISTRIBUTION OF ESSA PRODUCTS

**2.1. Focused Look Assessment Request Procedures.** Subject to the authority of AFSPC to organize, train, and equip CDA mission forces, and subject to the delegated authority of 24AF to command them and execute the mission, the following procedures and process flows (see Figure 2.1) are provided for the information of CDA users.

2.1.1. Organizations request Focused Look Assessments through their Wing OPSEC PMs to their MAJCOM, DRU, FOA OPSEC PM.

2.1.2. The AF, MAJCOM, DRU, FOA OPSEC PM forwards Focused Look Assessment requests to the 624 OC and courtesy copies to the 67 CW/WCC.

2.1.3. The 624 OC considers recommendations of the 67 CW, then validates and resolves conflicts between CDA requests based on the following priorities:

2.1.3.1. Priority 1: Military operations:

2.1.3.1.1. Priority 1A: Major operations and campaigns

2.1.3.1.2. Priority 1B: Special operations forces

2.1.3.1.3. Priority 1C: Peace Operations, crisis response or limited contingency operations

2.1.3.2. Priority 2: Special access programs or research, development, test and evaluation activities, and OPSEC Surveys:

2.1.3.2.1. Priority 2A: Existing special access programs

2.1.3.2.2. Priority 2B: Test and evaluations

2.1.3.2.3. Priority 2C: Research and development

2.1.3.2.4. Priority 2D: OPSEC Surveys

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

2.1.3.4. Priority 4: AF organizations participating in Joint Chiefs of Staff directed exercises

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

2.1.3.6. Priority 6: Baseline assessments

2.1.3.7. Priority 7: All other assessments

2.1.4. The 624 OC will incorporate threat information when resolving competing or determining overall priorities. (T-1).

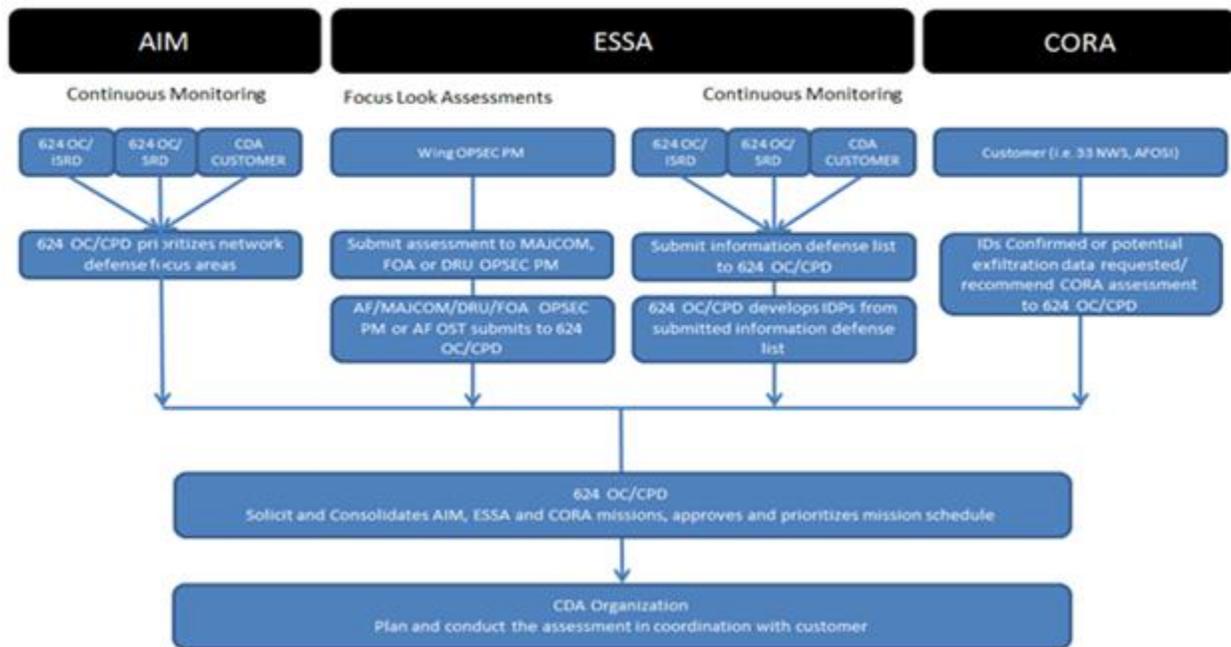
2.1.5. The 24 AF/CC or delegated representative approves assessment schedules. The approved tasking document constitutes authority for the organizations to operate.

2.1.6. The 624 OC then tasks the CDA units to execute the assessments. The 624 OC provides the CDA units at least 10 working days between task notification and mission

execution to allow CDA units to coordinate with the assessed organizations OPSEC PM or OPSEC PMs.

2.1.7. CDA units contact the AF, AF OST, MAJCOM, DRU, FOA OPSEC PM or Wing OPSEC PMs (as applicable) at the assessment location to plan the ESSA mission. Refer to paragraph 2.4 for further details.

**Figure 2.1. CDA Mission Request Process Flow**



**2.2. Distribution of ESSA Products.** This paragraph does not apply to reporting requirements covered in sections 3.2.2 through 3.2.7 of this instruction. In the circumstances described in those scenarios, the resulting notifications although derived from ESSA missions are not ESSA products, and operators should follow the procedures in the applicable section of this instruction, and other applicable regulations. All personnel will:

2.2.1. Limit distribution of products as stated in paragraph 2.2 of this instruction. **(T-1).**

2.2.2. Protect the rights and civil liberties of individuals who use monitored systems by complying with the procedures herein. Protect properly marked proprietary information as provided in Code of Federal Regulations, Title 48 *Federal Acquisition Regulations System*, Section 27.402. **(T-1).**

2.2.3. Use information in products only for official purposes, except as otherwise noted in paragraph 2.2 of this instruction. **(T-1).**

2.2.4. Do not use ESSA products to produce foreign intelligence or counterintelligence information. **EXCEPTION: CORA products as noted in 1.3.4.6 of this instruction. (T-1).**

2.2.5. Release ESSA products to opposing forces during exercises or evaluations only under the following conditions: **(T-1).**

2.2.5.1. Reports must maintain their identity as ESSA products. **(T-1).**

2.2.5.2. Do not identify or represent the products to be signals intelligence. (T-1).

2.2.5.3. Do not identify any communicating parties. (T-1).

2.2.5.4. Expressly state dissemination controls on each report. The exercise director determines dissemination. (T-1).

**2.2.6. Awareness and Training.** ESSA products can support Information Protection awareness and training efforts by providing real-world examples of exposed information and communications practices.

2.2.6.1. CDA units performing ESSA missions may provide extracts of reports and brief quotes of assessed communications. Communicating parties will not be identified in any way. (T-1).

2.2.6.2. 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. (T-1).

**2.2.7. Adverse or Disciplinary Personnel Actions.** Information obtained during an ESSA mission will not be used as evidence in a criminal prosecution without approval of SAF/GC. (T-0). Prior to drafting charges, installation level Staff Judge Advocates (SJA) will submit ESSA derived materiel they intend to use as evidence to 67 CW/JA for comment. (T-1). 67 CW/JA's legal review will be provided via command JA channels to AF/JAO and SAF/GCI for coordination. (T-1).

**2.3. ESSA Products.** All ESSA products are marked and protected at a minimum FOR OFFICIAL USE ONLY until possible disclosures are thoroughly evaluated and any weaknesses corrected. Classify and mark ESSA products according to security classification guides, DOD Manual (DODM) 5200.01, Volumes 2 and 4, *Information Security Program; Marking and Control Unclassified Information*, and current policy and guidance. Contact the unit security manager to receive Derivative Classification training prior to marking any document. This training is required IAW Presidential Executive Order 13526, Part 2 – Derivative Classification, Section 2.1.

**2.4. Types of ESSA Products.** There are two basic types of ESSA products, consisting of reports and transcripts. Paragraphs 2.4.1 through 2.4.2 of this instruction describe exceptions to the restrictions on the dissemination and retention of ESSA products. In the circumstances described in those exceptions, the resulting notifications are not ESSA products and operators should follow the procedures in Paragraph 3.2 and other applicable regulations.

2.4.1. **Reports.** ESSA reports provide operational commanders with near real-time reports of classified or critical information disclosures that may adversely affect U.S. (and allied/coalition) operations. Reporting formats should be tailored to meet the circumstances of the ESSA and the individual needs of the customer. Operational commanders should use these reports for evaluating the effectiveness of OPSEC countermeasures, 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. ESSA reports include; information protection alerts (IPA), immediate reports trend reports, and summary reports. ESSA reports are provided to all organizations effected whether the ESSA is a part of continuous monitoring or a Focused Look Assessment. ESSA

products are sent to those organizations that are impacted by the information disclosure, data loss, or vulnerability trend. **(T-1)**. At a minimum, a copy of all sanitized ESSA products will be sent to the HHQ OPSEC PM of all the affected organizations and the Air Force OPSEC Support Element (OSE) when the disclosing organization is scheduled for an OPSEC external assessment. **(T-1)**. Reports should not supply sufficient data to identify an individual to those elements. Reports may include short quotes, extracts, or sanitized email attachments as needed to clarify information, but not entire reproductions of communications. Trend and summary reports will include applicable threat information. Specific limited exceptions for authorized distribution and use of products with attribution are provided in 3.2. **(T-1)**.

2.4.1.1. An IPA is a shortened reporting format used to notify the customer of possible disclosures upon discovery during an ongoing assessment. These reports may contain information of value to hostile intelligence services, unclassified critical information, or information pertaining to the movement of high level distinguished visitors (DV). IPAs are ESSA products and should not be used to satisfy notification requirements for events that require full attribution as outlined in paragraph 3.2.2 through 3.2.7 of this instruction.

2.4.1.2. An immediate report provides time-critical information, force protection information, compromises of classified information, and/or mission critical information during exercise and real world operations.

2.4.1.3. Trend reports are issued at varying intervals e.g., whenever analysis uncovers a significant trend of damage and/or vulnerabilities. These reports may summarize and analyze damage and/or vulnerabilities covered in previous ESSA reports, CORA damage assessments, or OPSEC indicators in aggregate that uncover larger vulnerabilities. Trend reports may be labeled as ESSA, but may contain information from ESSA-derived as-well-as non-ESSA-derived sources. In cases where ESSA-derived information is cited in this report, it must be properly labeled as "ESSA-derived" information and adhere to other handling requirements identified in section 2.3, 3.2, and 3.3 of this instruction.

2.4.1.4. Summary reports are used to review all information gathered following a completed organization requested Focused Look Assessment. The summary report reviews all information put at risk or compromised and all information in aggregate used during the risk and damage assessments. This report is typically issued with 60 calendar days after the assessment is completed. Summary reports may be labeled as ESSA, but may contain information from ESSA-derived information as-well-as non-ESSA-derived sources. In cases where ESSA-derived information is cited in this report, it must be properly labeled as "ESSA-derived" information and adhere to other handling requirements identified in sections 2.3, 3.2 and 3.3 of this instruction.

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

2.4.2.1. Sanitized transcripts are furnished upon request of an organization. A sanitized transcript is a true representation of a communication, but will not contain PII, including sensitive PII, or information that could reasonably identify individuals (names, ranks,

specific duty positions, etc.). **(T-1)**. Sanitized transcripts are typically requested when a report reveals critical information disclosures that do not meet the criteria from sections 2.3. or 3.2.1. through 3.2.6 of this instruction.

2.4.2.2. Un-sanitized transcripts are true and complete representation of a communication(s). They are generated whenever criteria are met from sections 2.3 (as defined by the 67 CW/CC) or 3.2.1 through 3.2.5 of this instruction. When the criteria in any of paragraphs 3.2.1 through 3.2.5 are met, un-sanitized transcript may be attached to or included in other reports to streamline notifications when possible. An organization may request an un-sanitized transcript if they believe the communication meets the criteria in paragraph 3.3. An un-sanitized transcript includes both the sending and receiving communicator's information (if available). This type of transcript is the final product of the attribution process described in section 3.3 of this instruction.

2.4.2.3. Transcripts. Classify all transcripts (sanitized or un-sanitized) according to content. All markings for both classified and unclassified transcripts must be IAW DODM 5200.01, Volumes 2 and 4, *Information Security Program; Marking and Control Unclassified Information*. **(T-1)**.

## Chapter 3

### ESSA ATTRIBUTION AND UNIQUE REPORTING

**3.1. Release of ESSA Information.** Identifying information may be released as provided in Paragraph 3.2 of this instruction. In all other cases, do not release 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. At a minimum, include the three letter office of the offending organization. As long as the information in a product does not identify specific individuals as the source of the disclosure, a product may contain names, titles, or ranks when it is an integral part of the possible disclosure.

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

**3.2.1. Emergency Situations.** This section will apply if information threatening death, serious bodily harm, significant or intentional compromise of classified information, or major loss of property is obtained during an ESSA assessment. (T-3).

3.2.1.1. 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 effected organization, or other agency as necessary to resolve the emergency.

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

3.2.1.3. Complete identifying data may be released.

3.2.1.4. This is not ESSA information; therefore, this data does not appear in any ESSA product.

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

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

3.2.1.7. Within 24 hours of initial reporting, notify 67 CW/JA by message.

**3.2.2. Criminal, Foreign Intelligence, and Counterintelligence Information.** Information incidentally acquired during ESSA activities that directly relates to criminal, foreign intelligence, and counterintelligence information will be reported as follows: (T-1):

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

3.2.2.2. Complete identifying data may be released.

3.2.2.3. Although derived from ESSA activity, this data is not be included in any ESSA product.

3.2.2.4. Within 24 hours of initial reporting, notify 67 CW/JA by message. 67 CW/JA will promptly provide a legal review of the report to be forwarded via command JA channels to AF/JAO and SAF/GCI. (T-1).

3.2.3. **Classified Information.** This paragraph will apply for reporting purposes only. If information revealing a compromise or continuing threat of a compromise of classified information is obtained during the assessment, follow the reporting guidance within AFI 31-401, *Information Security Program Management*. If found within an assessed communication also:

3.2.3.1. Release only the minimum amount of data necessary to ensure prompt remedial action. Within the report briefly, summarize what was sent and its classification.

3.2.3.2. If an attachment is present, it may also be sent using secure means to the appropriate information protection office, OPSEC PM for evaluation. The information protection office is the first level of management for classified information.

3.2.3.3. 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 commander, network control officials, information protection office, OPSEC PM to facilitate the positive identification, containment, and remediation of compromised data or account from the network or information system.

3.2.4. **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 an ESSA product:

3.2.4.1. High-level DV movements, such as the President, Vice President, foreign heads of state or foreign ambassadors. Reportable data also includes information pertaining to specific dangerous situations and/or a threat, plan, or attempt to physically harm or kidnap certain individuals, as described in AFI 71-101V2, Attachment 3. Report this information to the local AFOSI detachment of the CDA unit conducting the assessment, who in-turn reports this information to the local AFOSI detachment at the assessed location.

3.2.4.2. Derivatively classify products utilizing the applicable security classification guide or source document. Specific itineraries may carry a higher classification based on trip sensitivity. For information regarding classification, guides contact the information protection office.

3.2.5. **Vulnerabilities to Unclassified Government Owned/Leased Networks and/or Databases.** If vulnerabilities to unclassified government owned or leased networks or databases are discovered in the course of an ESSA assessment, immediately release full header information (to, from and cc lines or sending/receiving addresses; dates/ times; and subject line) to the appropriate commander, network control officials, information protection offices, OPSEC PM to facilitate the positive identification, containment, and remediation of compromised data or account from the network or information system. Vulnerabilities are defined as a release of user credentials of government owned or operated systems, network topology data, compromises of PII, or other information that may allow an adversary to attack or exploit AF networks. **EXCEPTION:** Communications to and from various help

desks or Cybersecurity offices to report and resolve network or systems issues are not to be reported.

**3.2.6. Reportable Breach of PII.** Breaches of PII must be reported as directed in AFI 33-332, *The Air Force Privacy Program and Civil Liberties Program*, paragraph 9.3. A reportable breach is identifying information specific to an individual that has been sent unencrypted from or to an AFIN account to or from a commercial server in violation of AF policy. In such cases, report the names of all parties involved in the potential breach, the facts, and the circumstances around the potential breach to the appropriate HHQ Privacy Act PM, OPSEC PM Office, and/or US-CERT, as the situation requires.

**3.2.7.** Commanders seeking an unsanitized transcript which does not fall within the parameters above may request one from 67 CW/CC, with a copy to 67JA. The request must explain the need for the unsanitized product, including how the proposed use would fit within the limitations of NTISSD 600 and DODI 8560.01, *COMSEC Monitoring and IA Readiness Testing*, paragraph 4.1. The 67CW/ JA in consultation with 24AF/JA will review the request and unsanitized ESSA product and they will make a recommendation to 67 CW/CC whether the request is consistent with the NTISSD and the DODI. If 67 CW/CC recommends release of the transcript, the analysis and his recommendation will be forwarded to SAF/GC via AFSPC/A3 and JA, for SAF/GC approval. **(T-3)**. Except as provided in paragraph 3.2, of this instruction unsanitized ESSA transcripts may not be released without approval from SAF/GC.

**3.3. Assessment Preparation.** When CDA teams conducting ESSA missions are unable to conduct an assessment via remote operations the CDA teams may need to deploy to the tasked assessed location. The CDA team may require assistance from the assessed organization well before the actual start date of the ESSA assessment mission. The assessed organizations OPSEC PM will interface with the CDA team conducting the ESSA mission and other base agencies. **(T-2)**. The following are typical actions needed to prepare for an assessment:

3.3.1. Gain familiarity with ESSA objectives and methods.

3.3.2. Ensure senior leadership is advised of ESSA activities.

3.3.3. Provide security classification guides.

3.3.4. Upon request, provide operational orders, phone books, plans, operating instructions, or other mission related documents.

3.3.5. For telephone monitoring, generate an initial list of phone numbers, along with their associated flight, office, division symbol or abbreviation 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 and defense counsel offices, and chapels/chaplains will not be selected for assessment. **(T-0)**.

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

**3.4. Team Travel and Funding.** When teams are unable to conduct ESSA missions via remote operations, the teams may need to deploy to the assessed location. If the CDA team has to conduct an ESSA mission at the assessed organization's location due to lack of technology, it is

the responsibility of the CDA unit to fund the CDA team's travel. If the assessed organization requests an ESSA mission on location, it is the responsibility of the assessed organization to fund the travel of the CDA assessment team. (Note: The 624 OC determines if a lack of technology is responsible for team deployment. The assessed unit may appeal to 67 CW/CC or AFSPC/CC if they disagree with the 624 OC's decision.) The following are specific to an on-site assessment, and supplement the actions listed above:

3.4.1. Coordinate a work area and secure storage facility for the CDA team performing the ESSA mission.

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

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

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

**3.5. Quality Control (QC).** QC is an integral part of accomplishing and managing the mission and is necessary to ensure all aspects of ESSA operations are the most professional possible. QC checks identify strengths and weaknesses of training processes, ensures customers receive professional and quality products, and serves as a feedback tool through trends analysis to share training strengths and correct training deficiencies.

## Chapter 4

### NOTICE AND CONSENT PROCEDURES

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

**4.2. Telephone Directories.** Prominently display the following notice and consent statement on the front cover of printed telephone directories and/or first page of electronic telephone directories. If the telephone directory is embedded in a base information guide, this notice must precede the telephone directory portion of the base guide:

**4.2.1. “DO NOT DISCUSS CLASSIFIED INFORMATION ON UNSECURE TELEPHONES. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES.”**

**4.2.1.1. “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.”** NOTE: For the purpose of notice and consent, unofficial organizational charts and rosters are not considered telephone directories

**4.3. Telephones.** The DD Form 2056, *Telephone Monitoring Notification Decal*, must be affixed on the front of all official telephones, including Voice over Internet Protocol (VoIP) phones. (T-0). 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. Replicated DD Form 2056 are acceptable as long as they have the exact statement as follows:

**4.3.1. “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.”**

**4.4. Facsimile Machines and Multi-Function Devices.** Both of the following actions are required to notify users of official facsimile machines and unclassified multi-function print devices with facsimile and/or electronic communications capabilities enabled:

**4.4.1.** The DD Form 2056 must be affixed on all facsimile machines and multi-function print devices. (T-0). Locally generated notice and consent stickers are permitted as long as the wording matches the DD Form 2056 exactly or the exact statement listed in paragraph 4.3 of this instruction.

**4.4.2.** Use the AF Form 3535.

**4.5. Information Systems.** Put users of unclassified AF information systems (e.g., any electronic device connecting to the AFIN, stand-alone electronic devices, and portable electronic devices) on notice that their use constitutes consent to monitoring.

4.5.1. The notice and consent log-on banner, Attachment 2, must be installed on all computers. (T-2). 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 to install the complete notice and consent log-on banner cited in Attachment 2 of this instruction, the MAJCOM or DRU/A6 may authorize the following:

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

4.5.2.1.1. **“I’ve read & consent to terms in IS user agreement. ”**

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 Cybersecurity office or designated representative until six months after the user no longer requires access to the system. (T-0).

4.5.2.3. If the system is not capable of complying with paragraph 4.5.2.1, a DD Form 2056 must be affixed on all computer monitors and video display screens.

**4.6. Private or Intranet Web Home pages.** Prominently display the exact notice and consent banner specified in Attachment 2 of this instruction on the first page of all private and intranet web home pages (to include SharePoint sites); the banner is not required on subsequent pages. Hyperlinks to the notice and consent statement do not meet the requirement as it pertains to private/intranet web pages. Banner pop-ups are authorized ONLY when access to the page requires the user to press a key/button, thereby demonstrating acceptance of the banner provisions.

4.6.1. Notice and consent requirements do not apply to 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 will 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, cell phones, smartphones, tablets, satellite phones, and hand-held radios/land mobile radios (LMRs)). Refer to AFMAN 33-282, for more information on PEDs. These devices, excluding LMRs and PEDs identified in paragraph 4.7.1.1 of this instruction, must comply with the requirements in paragraph 4.5 of this instruction to the extent technically possible..

4.7.1. All PED users must sign an AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement*. LMR users are exempt from this requirement if the LMR has a DD Form 2056 attached to it. The signed form will be retained by the organizational

Cybersecurity office or designated representative for a minimum of six months after the device has been returned to the issuing office. **(T-1)**.

4.7.2. PEDs and LMRs that cannot display the abbreviated Notice and Consent banner requirement must have a DD Form 2506 attached, unless the organization commander has Force Protection and/or OPSEC concerns based on the local operating environment IAW AFI 10-701, Operations Security (OPSEC), or unless the PED/LMR is too small to accommodate a DD Form 2506. Small locally generated DD Forms 2056 are authorized if necessary to fit on a PED or LMR. If Force Protection/OPSEC concerns preclude use of a DD Form 2506, then members issued an LMR must sign and AF Form 4433.

**4.8. Other Information Technology.** Any telecommunication devices not otherwise referenced in this chapter must have a signed AF Form 4433 or AF Form 4394 on file. The signed forms will be retained by the Organizational Cybersecurity office or the designated representative for a minimum of six months after the device has been returned to the issuing office. **(T-1)**.

**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. **(T-1)**. Optional methods to provide users with legally sufficient notice of their use of electronic communications 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 organizations for dissemination to unit personnel.

4.9.2. Addressing notice and consent provisions to newcomers during in-processing, periodic 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 electronic communications systems users are aware that using these systems and devices constitutes consent to electronic communications monitoring.

**4.10. Notice and Consent Certification Process.** This section describes the biennial certification, by SAF/GC, that users of AF electronic communication 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 electronic communications monitoring and cybersecurity readiness testing procedures, training processes, and user notification procedures on a biennial basis, as mandated by DODI 8560.01.

4.10.1. HQ AFSPC/A2/3/6, 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. **(T-1)**.

4.10.3. The Wing Cybersecurity office will at a minimum, complete and document the actions outlined in this instruction. **(T-1)**.

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 Cybersecurity 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 4 of this instruction.

4.10.3.1.1. The Notice and Consent Checklist Attachment 5, is provided to assist with completing the notice and consent summary package and determining which attachments are required to be included.

4.10.3.1.2. The Wing Cybersecurity office 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.

4.10.3.1.3. Only submit summary packages electronically as a single PDF document 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 in paragraph 1 of this instruction. FOAs, DRUs, and tenants will be addressed per the following: **(T-1)**.

4.10.3.2.1. FOAs and DRUs located on a host base report their notice and consent compliance through the host Wing Cybersecurity office.

4.10.3.2.2. FOAs and DRUs not located on a host base report their notice and consent compliance as a Wing Cybersecurity office.

4.10.3.2.3. All other tenant wings or organizations report their notice and consent compliance through the host installation Wing Cybersecurity office.

4.10.4. The Installation SJA reviews the summary and attached documentation and provides written review (see Attachment 4 of this instruction 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 electronic communication 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 will be returned for corrective action. If the package is determined to be legally sufficient, the Wing Cybersecurity office includes the SJA’s written determination as part of the certification package. Upon endorsement, the installation SJA will forward the summary back to the Wing Cybersecurity 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 of each even-numbered fiscal year.

4.10.5. MAJCOM/DRU/FOA /A6, in coordination with HQ AFSPC/A2/3/6, 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.

4.10.5.1. Validates bases/wing/FOA/tenant units identified in the precious SAF/GC certification memo are correct, providing updates to AFSPC/A2/3/6 as needed.

4.10.5.2. Ensures AFSPC/A2/3/6 has current contacts for each Wing Cybersecurity office.

4.10.6. MAJCOM/DRU/FOA/ SJA reviews the summary, attached documentation for legal compliance, and provides a written review (see Attachment 4 of this instruction for MAJCOM SJA 2nd endorsement format). If the MAJCOM SJA determines the documentation is deficient in any of the requirements, the package will be returned to the Wing Cybersecurity office 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 Cybersecurity office.

4.10.7. Following host base wing or communications commander signature, installation SJA endorsement and MAJCOM or DRU/SJA endorsement, the Wing Cybersecurity office sends the installation summary package, with supporting documentation, as a single PDF file for review to HQ AFSPC/A2/3/6 no later than 15 May of each even-numbered fiscal year. Additionally, Wing Cybersecurity office will send an informational copy of only the summary letter to the MAJCOM and DRU/A6. **(T-2)**.

4.10.8. HQ AFSPC/JA ensures all AF facilities submit inputs in order to receive biennial certification according to Table 4.1, Notice and Consent Certification Schedule. HQ AFSPC/A2/3/6 reviews all summary packages for required content and correct format. Packages requiring corrections and/or clarifications are returned to the responsible Wing Cybersecurity office. Packages that are determined to be complete and in the correct format are forwarded to HQ AFSPC/JA for final endorsement before submission to SAF/GC.

4.10.9. Any deficiencies noted by HQ AFSPC/JA are returned to the responsible Wing Cybersecurity office for correction. When necessary for compliance, coordination through the MAJCOM Cybersecurity office is required to ensure installation Wing Cybersecurity offices understand and accomplish necessary correction actions. Once corrected, HQ AFSPC/JA will endorse all summary packages and submit electronically to SAF/GC by 15 July of each even-numbered fiscal year. **(T-1)**.

4.10.10. SAF/GC certifies that there has been sufficient notice that the use of DOD electronic communication 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 HQ AFSPC/A2/3/6 by 1 September of each even-numbered fiscal year listing all installations approved for authorized monitoring activities. Upon receipt of the certification listing, HQ AFSPC/A2/3/6 forward copies to an authorized monitoring agency as prescribed by DODI 8560.01. HQ AFSPC/A2/3/6 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 are to 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.

**4.11. 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**

<b>Even Year Date</b>	<b>Office</b>	<b>Action</b>
Mid-January	HQ AFSPC/A2/3/6	Release heads-up message to MAJCOM, DRU, FOA/A6s announcing start of certification cycle
Mid-January – 15 February	MAJCOM, DRU, FOA/A6, Wing Cybersecurity office	Validate all installations and GSUs from the previous cycle certification letter and report changes to HQ AFSPC/A2/3/6 with detailed
Early February	HQ AFSPC/A2/3/6	Conduct telecon w/MAJCOM, DRU, FOA/A6s and Wing Cybersecurity offices - Initiates
Early February	HQ AFSPC/A2/3/6	(If necessary) Send new procedures and/or guidance to all Wing Cybersecurity offices with courtesy copy to MAJCOM, DRU, FOA/A6s
Early February - After Telecon	HQ AFSPC/A2/3/6	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
Early Feb – 15 March	Wing Cybersecurity office / Installation JA	Sends Notice and Consent Certification Summary package to Installation SJA for review. Sends endorsement to Wing Cybersecurity office
15 – 30 March	Wing Cybersecurity office / MAJCOM JA	Sends Notice and Consent Certification Summary package to MAJCOM SJA for review. Sends endorsement to Wing Cybersecurity office
NLT 1 April	Wing Cybersecurity office	Submits summary package as single PDF portfolio to HQ AFSPC/A2/3/6 for review
NLT 1 April	Wing Cybersecurity office	Notify MAJCOM, DRU, FOA A6 that package was submitted for review
1 April – 15 June	HQ AFSPC/A2/3/6	Reviews summary packages, coordinates corrections with MAJCOM/A6, Wing Cybersecurity office and sends packages to HQ AFSPC/JA for review

15 June – 15 August	HQ AFSPC/JA	Reviews summary packages, coordinates corrections with MAJCOM/A6, HQ AFSPC/A2/3/6, endorses and sends packages to SAF/GC for review
15 Sep	SAF/GC	Reviews summary packages and provides HQ AFSPC/A3/A6/JA with certification letter listing bases approved for monitoring
Before 30 Sep	HQ AFSPC/A2/3/6	Sends SAF/GC certification letter and final summary packages to each Wing Cybersecurity office

JOHN W. RAYMOND, Lt Gen, USAF  
Deputy Chief of Staff, Operations

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

- DODD 4500.54, *DOD Foreign Clearance Program (FCP)*, 28 December 2009
- DODM 5200.01, Vol 2, *DOD Information Security Program; Marking and Control Unclassified Information*, 24 February 2012
- DODD 5205.02, *DOD Operations Security (OPSEC) Program*, 20 June 2012
- DODM 5205-02-M, *DOD Operations Security (OPSEC) Program Manual*, 3 November 2008
- DODD 7050.06, *Military Whistleblower Protection*, 23 July 2007
- DODI 8500.01, *Cybersecurity*, 14 March 2014
- DODI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing*, 9 October 2007
- DODI 8550.01, *DOD Internet Services and Internet-based Capabilities*, 11 September 2012
- 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
- AFPD 10-17, *Cyberspace Operations*, 31 July 2012
- AFI 10-401, *Air Force Operations Planning and Execution*, 7 December 2006
- AFI 10-701, *Operations Security (OPSEC)*, 8 June 2011
- AFI 10-1701, *Command and Control (C2) For Cyberspace Operations*, 5 March 2014
- AFI 11-260, *Tactics Development Program*, 15 September 2011
- AFI 31-401, *Information Security Program Management*, 1 November 2005
- AFI 33-200, *Information Assurance (IA) Management*, 23 December 2008
- AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, 23 December 2008
- AFI 33-332, *The Air Force Privacy and Civil Liberties Program*, 5 June 2013
- AFI 33-360, *Publications and Forms Management*, 25 September 2013
- AFI 71-101, Volume 2, *Protective Service Matters*, 18 November 2002
- AFI 90-301, *Inspector General Complaints Resolution*, 23 Aug 2001
- AFMAN 33-152, *User Responsibilities, and Guidance for Information Systems*, 1 June 2012
- AFMAN 33-282, *Computer Security (COMPUSEC)*, 27 March 2012
- AFMAN 33-363, *Management of Records*, 01 March 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 847, *Recommendation for Change of Publication*

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

AF Form 4433, *US Air Force Unclassified Wireless Mobile Device User Agreement*

***Abbreviations and Acronyms***

**AF**—Air Force (when used on forms)

**AFI** —Air Force Instruction

**AFMAN** —Air Force Manual

**AIM** —Active Indicator Monitoring

**ANG**—Air National Guard

**AFR**—Air Force Reserve

**CDA** —Cyberspace Defense Analysis

**COMSEC**—Communications Security

**CORA** —Cyber Operations Risk Assessment

**DOD**—Department of Defense

**DODD** —Department of Defense Directive

**DODI** —Department of Defense Instruction

**DODM** —Department of Defense Manual

**DRU**—Direct Reporting Unit

**DTS-W** — Defense Telecommunications Service-Washington

**ESSA** —Electronic Systems Security Assessment

**FOA**—Field Operating Agency

**GSU**—Geographically Separated Unit

**IbC**—Internet-based Capability

**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  
**PPI**—Personal Privacy Information  
**PM**—Program Manager  
**RDS**—Records Disposition Schedule  
**T-0**—Tier 0 Waiver Authority  
**T-1**—Tier 1 Waiver Authority  
**T-2**—Tier 2 Waiver Authority  
**T-3**—Tier 3 Waiver Authority  
**WRA**—Web Risk Assessment  
**WCO**—Wing Cybersecurity office  
**WS**—Weapon System

### *Terms*

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

**Active Indicator Monitoring (AIM)**—Identifies activities that potentially expose AF networks, systems and personnel to increased risk as a result of the action or inaction of an authorized user who discloses AF system credentials, accounts, exploitable network configuration information or PII.

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

**Cyberspace Defense Analysis (CDA)**—The AF weapon system managed by AFSPC and refers to the resources, tools, and manpower required to conduct the monitoring, collection, and analysis of information content transmitted across DOD electronic communication systems.

**Cyber Operations Risk Assessment**— The analysis of data compromised through intrusions of the Air Force Information Network (AFIN) with the objective of determining the associated impact to operations resulting from data loss to adversaries.

**Cybersecurity**— Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation. (Replaces Information Assurance IAW DODI 8500.01, 14 March 2014)

**Electronic Systems Security Assessment (ESSA)**— The monitoring, collection, and analysis of information content transmitted across DOD electronic communication systems. ESSA products help evaluate an organization’s OPSEC posture and determine the amount and type of information available to adversary collection entities. (Formerly the Telecommunications Monitoring and Assessment Program (TMAP).

**Home page**— 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 Protection (IP)** — 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 critical 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.

**Peace Operations** — A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance.

**(JP 1-02) Personal Digital Assistant (PDA)** — Devices such as Palm Pilot®, Cassiopeia®, Blackberry®, etc.; a PDA is one type of PED (see below).

**Personally Identifiable Information (PII)** —A combination of Personal Identifier and Personal Information: **Personal Identifier**—A name, number, or symbol that is unique to an individual and can be used to trace an individual identity, usually the person's name or social security number.

**Personal Information**—Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., SSN; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as *personally identifiable information* (PII) (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, place of birth, mother's maiden name, or biometric records, including any other PII which is linked or linkable to a specified individual).

**Personal Privacy Information (PPI)** —Unique to ESSA and CDA. Any item, collection, or grouping of information about an individual's private or personal affairs which are not job related. This includes personal financial matters, social behavior, physical condition, or any other information that could defame a person's character, integrity, or family.

**Personnel Action** — Any action taken on a member of the armed forces that affects or has the potential to affect (for example a threat) that military 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 and DODD 7050.06)

**Popup 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.

**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.

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

**Tier Waiver Authorities** — Tier Waiver Authority is based on consequence of non-compliance and approval authority (AFI 33-360, Table 1.1).

**T-0** — Waiver Authority is external to the Air Force (e.g. Executive Order, DOD, Joint Staff, Combatant Commands).

**T-1** — Waiver Authority is MAJCOM/CC (delegable no lower than the MAJCOM Director), with the concurrence of the publication's Approving Official.

**T-2** — Waiver Authority is MAJCOM/CC (delegable no lower than MAJCOM Director).

**T-3** — Waiver Authority is Wing/CC

**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 un-sanitized.

**Un-sanitized Transcript** -- Is a verbatim reproduction of an assessed communication including any identifying 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.

**Web Risk Assessment** —The assessment of information posted on AF 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.

**Attachment 2****STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER**

**A2.1. Use this banner for desktops, laptops, and other devices** accommodating banners of 1300 characters. The banner will 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."

**A2.2. You are accessing a U. S. Government (USG) Information System (IS)** that is provided for USG-authorized use only.

**A2.3. By using this IS** (which includes any device attached to this IS), you consent to the following conditions:

A2.3.1. 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.

A2.3.2. At any time, the USG may inspect and seize data stored on this IS.

A2.3.3. 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.

A2.3.4. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

A2.3.5. 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.

A2.3.5.1. “\*OK”

**A2.4. [For Blackberries and other PDAs/PEDs with severe character limitations:]**

A2.4.1. “\*\*I've read & consent to terms in IS user agreement”.

### Attachment 3

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

**A3.1. By signing this document** you acknowledge and consent that when you access Department of Defense (DOD) information systems:

**A3.2. 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.

**A3.3. You consent to the following conditions:**

**A3.4. 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.

**A3.5. 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.

**A3.6. 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.

**A3.7. 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:

**A3.8. 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.

**A3.9. 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.

**A3.10. 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.

**A3.11. 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.

**A3.12. 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.

**A3.13. 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.

**A3.14. 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.

**A3.15. 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 4

## NOTICE AND CONSENT MEMORANDUM WITH 1ST AND 2ND IND

Figure A4.1. Notice and Consent Memorandum with 1st and 2nd Ind.

DATE

MEMORANDUM FOR: [Supporting Legal Office]

FROM: (Insert address information of organization submitting summary package)

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 unclassified DOD electronic communication systems and devices that using those systems constitutes consent to electronic communications monitoring for (insert installation) including all tenants, Field Operations Agencies, and Direct Reporting Units, located on this installation and the following Geographically Separated Units (GSUs) located off this installation: (list all GSUs).

Note: (Include if applicable) The following GSUs were included in the installation's previous biennial summary package, but are no longer included: (insert GSUs and detailed explanation for each).

a. The current installation telephone directory, dated (insert date), is maintained in (insert one: printed copy only; electronic version only; both printed copy and electronic version), and includes the notice and consent statement on the front cover/first page as required by AFI 10-712, paragraph 4.2. A copy/screenshot of the first/cover page is attached.

Note: (For installations where the AF is not the authority over the telephone directory (i.e., joint bases) or a directory does not exist, use the following statement in lieu of the previous paragraph: The AF does not maintain an installation telephone directory for XXX AFB.)

b. All official telephones have been inspected to verify a DD Form 2056 is affixed as required by AFI 10-712, paragraph 4.3. Decals were immediately applied to all non-compliant telephones. Hence, all official telephones have the DD Form 2056 affixed as of the date of this report.

c. All official unclassified facsimile (fax) machines and multi-function print devices have been inspected to verify a DD Form 2056 is affixed as required by AFI 10-712, paragraph 4.4. Decals were immediately applied to all non-compliant devices. Hence, all fax machines and multi-function print devices have the DD Form 2056 affixed as of the date of this report. d. All fax cover sheets have been inspected to verify only the AF Form 3535 is in use as required by AFI 10-712, paragraph 4.4. As of the date of this report, all fax cover sheets 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 unclassified information systems including, but not limited to networked, servers, stand-alone, and portable computers, servers, switches, routers, and any other functional system able to record, store, or transmit information. The banner is automatically displayed upon boot-up or initial log-on for the information system regardless of the access method. The banner was immediately installed on all non-compliant information systems or remediated as required by AFI 10-712, paragraph 4.5. Hence, all information systems are notice and consent compliant as of the date of this report. A representative sample of logon banners and locally generated labels (if used) are attached.

f. The current notice and consent banner is prominently displayed on all unit private/intranet web home pages as required by AFI 10-712, paragraph 4.6. A representative sample is attached.

g. All individuals issued a DOD owned Portable Electronic Device (PED) have signed an AF Form 4433 that is maintained on file with the organizational Cybersecurity office or designated representative for a minimum of six months after the device has been returned to the issuing office. Additionally, all PEDs have a DD Form 2056 affixed as required by AFI 10-712, paragraph 4.7.2. Hence, all PEDs are notice and consent compliant as of the date of this report.

h. All LMRs have either a DD Form 2056 attached or a signed AF Form 4433 on file with the Base LMR issuing authority or designated representative for a minimum of six months after the device has been returned to the issuing office.

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

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

4 Attachments:

1. Printed Telephone Directory (front cover) if applicable
2. Electronic Telephone Directory (print screen/first page) if applicable
3. Information System Notice and Consent Banner (print screen/representative sample)
4. Unit Private/Intranet Web Home page (print screen/representative sample)

1st Ind, JA, xx Apr xx

TO: 123d CS

In accordance with AFI 10-712, *Cyberspace Defense Analysis Operations (CDA) and Notice and Consent Process*, I have determined the notification actions outlined in your summary letter are sufficient to provide reasonable notice to all personnel using DOD electronic communication systems that such use constitutes consent to electronic communications monitoring.

LAWYER B. JUSTICE, Lt Col, USAF Judge Advocate

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

TO: 123 CS

In accordance with AFI 10-712, *Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process*, I have determined the notification actions outlined in your summary letter are sufficient to provide reasonable notice to all personnel using DOD electronic communication systems that such use constitutes consent to electronic communication monitoring.

JUSTICE LAWYER, Lt Col, USAF Judge Advocate

## Attachment 5

## NOTICE AND CONSENT CHECKLIST

Table A5.1. Notice and Consent Checklist

MANDATORY ACTIONS CHECK ALL ITEMS FOR COMPLIANCE	YES	NO	N/A
<p><b><u>1. Organizations:</u></b>            Have checklist items 2-8 below been answered for all organizations on the installation (including all tenants, FOAs, and DRUs) and all GSUs located off the installation?            Ensure all GSUs are listed in paragraph 1 of the installation's summary package</p>			
<p><b><u>2. Installation Telephone Directories:</u></b>            Does the installation have an AF maintained printed telephone directory?             Does the installation have an AF maintained electronic telephone directory?             Does the AF maintained installation telephone directory printed and/or electronic, contain the notice and consent statement from AFI 10-712, paragraph 4.2?   <u>Attachments (as required)</u>            1. Printed Telephone Directory (front cover) if applicable            2. Electronic Telephone Directory (print screen/first page) if applicable</p>			
<p><b><u>3. Telephones:</u></b>            Do all telephones (including STEs) have a DD Form 2056 affixed as required by AFI 10-712, paragraph 4.3?</p>			
<p><b><u>4. Facsimile Machines (FAX) and Multi-Function Devices (MFD):</u></b>            Do all facsimile machines and transmission enabled MFDs have a DD Form 2056 affixed as required by AFI 10-712, paragraph 4.4?</p>			
<p><b><u>5. FAX Cover Sheets:</u></b>            Is the AF Form 3535 or locally generated fax cover sheet used for all fax transmissions as required by AFI 10-712, paragraph 4.4?</p>			

<p><b><u>6. Information System Notice and Consent Banner:</u></b>  <b>Do all information systems display the required current log-in banner in full view or require the user to scroll through the entire banner before requiring user acknowledgement to proceed?</b></p> <p><b>If system limitations exist, has the abbreviated banner been installed or notice and consent label affixed as required by AFI 10-712, paragraph 4.5?</b></p> <p><u>Attachments (as required)</u>          3. Information System Notice and Consent Banner (print screen/representative sample, minimum 1 per device category)</p>			
<p><b><u>7. Private/Intranet Web Home pages:</u></b>  <b>Is the current notice and consent banner prominently displayed on all unit private/intranet web home pages or banner pop-up requiring user action demonstrating provision acceptance as required by AFI 10-712, paragraph 4.6?</b></p> <p><u>Attachments (as required):</u>          4. Unit Private/Intranet Web Home page (print screen/representative sample, minimum 10%)</p>			
<p><b><u>8. Portable Electronic Devices (PEDs):</u></b>  <b>Have all PED users signed an AF Form 4433?</b></p> <p><b>Have all signed AF Form 4433s been properly maintained as required by AFI 10-712, paragraph 4.7.1?</b></p> <p><b>Have all PEDs been labeled with a DD Form 2056 as required by AFI 10-712, paragraph 4.7.2?</b></p>			
<p><b><u>9. Attachments:</u></b>  <b>Have all required attachments been added to the installation's summary package?</b></p> <p><b>Are all attachments labeled and in the correct order?</b></p> <p><u>Attachment Listing:</u>          1. Printed Telephone Directory (front cover) if applicable          2. Electronic Telephone Directory (print screen/first page) if applicable          3. Information System Notice and Consent Banner (print screen/representative sample)          4. Unit Private/Intranet Web Home page (print screen/representative sample)</p>			

<p><b><u>10. Wing/Communication’s Squadron (CS) Commander:</u></b>  <b>Has the Wing/CS Commander reviewed and signed the installation’s summary package?</b></p>			
<p><b><u>11. INSTALLATION JA:</u></b>  <b>Has the installation summary package been endorsed by the installation JA stating legally sufficient notification has been provided to all personnel using DOD telecommunication systems that such use constitutes consent to electronic communication monitoring?</b></p>			
<p><b><u>12. MAJCOM/DRU/FOA JA:</u></b>  <b>Has the installation summary package been endorsed by the MAJCOM/DRU/FOA JA stating legally sufficient notification has been provided to all personnel using DOD telecommunication systems that such use constitutes consent to electronic communication monitoring?</b></p>			
<p><b><u>13. INSTALLATION IA OFFICE:</u></b>  <b>Does the installation summary package demonstrate complete notice and consent compliance as required by AFI 10-712, chapter 4?</b></p> <p><b>Has the installation summary package, including required attachments and endorsements, been compiled into a single PDF file for submission?</b></p> <p><b>Has the installation summary package been submitted to HQ AFSPC/A2/3/6 by 15 May deadline?</b></p>			