*BY ORDER OF THE*
*SECRETARY OF THE AIR FORCE*

*AIR FORCE INSTRUCTION 14-104*

*5 NOVEMBER 2014*

***Intelligence***

# *OVERSIGHT OF INTELLIGENCE ACTIVITIES*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

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

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

OPR: AF/A2ZS

Certified by: AF/A2Z
(Mr. Joseph D. Yount)

Supersedes: AFI 14-104, 23 April 2012

Pages: 26

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations* and is consistent with Executive Order (EO) 12333 (part 2), *United States Intelligence Activities*; Department of Defense (DoD) Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*; DoD Directive, and (DoDD) 5240.1, *DoD Intelligence Activities*. It states the requirements for United States Air Force (AF) intelligence oversight activities and describes mandatory intelligence oversight-associated training requirements for AF components that conduct intelligence activities. It also details how to identify, investigate, and report in the event of possible Intelligence Oversight (IO) violations. In this publication, the term "intelligence" refers to intelligence and counterintelligence units and associated activities. This publication does not apply to criminal investigative activities. For purposes of this publication, the National Guard Bureau is considered to be a major command (MAJCOM). This instruction applies to all AF, Air Force Reserve Command(AFRC) and Air National Guard (ANG) [in Title 10 or Title 32 (U.S.C.) status when assigned or attached to intelligence units or staffs]; and civilian personnel including, but not limited to, civil service, contract, consultants, and Host Nation employees engaged in or performing intelligence-related activities. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. IAW Air Force

Instruction (AFI) 33-360, *Publications and Forms Management*, tier levels ("T-0, T-1, T-2, T-3") following compliance statements determine the appropriate authority from which waivers must be requested. 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.

## *SUMMARY OF CHANGES*

This publication has been substantially revised and must be completely reviewed. It adds risk factors, known as "tiers" to tasks assigned to organizations below MAJCOM level to depict the assessed risk of non-compliance. Additional changes within this rewrite include: revising IO responsibilities, removing annual reporting requirements IAW ATSD (IO) guidance, and updating Proper Use Memorandum (PUM) guidance. Annual training requirements have also been substantially revised to eliminate unnecessary duplication of training. AF members assigned to non-AF agencies are now eligible for exemption from the AF IO computer based training (CBT) if the non-AF agency requires completion of its formal IO training.



## 1. Overview.

1.1. **Purpose.** US decision-makers need information about the capabilities, intentions, and activities of foreign governments and non-state actors in order to make decisions about national defense and foreign relations. IO involves a balancing of two fundamental interests: Obtaining the intelligence information required to protect national security while protecting individual rights guaranteed by the Constitution and outlined within the laws of the United States (US). The primary objective of the AF IO Program is to mitigate infringement upon the rights of US persons by ensuring that intelligence personnel at all levels understand IO responsibilities.

1.2. **Collection.** Information is considered "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of official duties. Data acquired by electronic means is "collected" only after it has been processed into intelligible form.

1.3. **Scope.**

1.3.1. This instruction applies to all AF active duty, AFRC, and ANG intelligence units, staff organizations, civilian-contracted organizations and non-intelligence organizations that perform intelligence-related activities (e.g., Eagle Vision units and cyberspace activities) that could collect, analyze, process, retain, or disseminate information on US persons.

1.3.2. This instruction does not apply to criminal investigations conducted by the Air Force Office of Special Investigations (AFOSI). Reference AFI 71-101 Volume 1, *Criminal Investigations.*

**2. Roles and Responsibilities.**

2.1. **Inspector General (SAF/IG).** Compiles inputs from SAF/GC, AF/A2, SAF/IGX and MAJCOM/Field Operating Agency (FOA)/Direct Reporting Unit (DRU) Inspectors General to provide quarterly reports to the Assistant to the Secretary of Defense for Intelligence Oversight [ATSD (IO)]. Has access to all material necessary to perform responsibilities. Chairs the AF IO Panel and has voting privileges on the panel.

2.2. **Air Force Intelligence Oversight Panel.** Is the lead AF IO advisory group that discusses the legality and propriety of reported AF intelligence activities and reviews current AF IO policy to ensure it aligns with US and DoD guidance. Meets, as required, and recommends changes to current AF IO policy or procedures to mitigate future IO concerns. Includes SAF/IG (chair), SAF/GC, AF/A2 and AF/JA.

2.3. **Secretary of the Air Force, General Counsel (SAF/GC).** Legal Counsel for Air Force IO issues. Provides legal opinions and advice to intelligence components in coordination with the servicing legal office responsible for advising the intelligence component on questions of legality or propriety as appropriate. Provides input to SAF/IG in preparation of quarterly reports to the ATSD (IO). Has access to all material necessary to perform their responsibilities. Voting member of the IO Panel.

2.4. **Deputy Chief of Staff (DCS), Intelligence, Surveillance, and Reconnaissance (ISR) (AF/A2).** Develops AF guidance and policy to ensure the proper supervision and control of AF intelligence activities and oversight. Coordinates with the ATSD(IO), the SAF/IG, and the SAF/GC on IO matters. Provide IO inspection requirements to SAF/IG for inclusion in AFI 90-201, *The Air Force Inspection System* (AFIS). Voting member of the IO Panel. Appoints an IO monitor to manage intelligence oversight policy and concerns on behalf of AF/A2.

2.5. **The Judge Advocate General (AF/JA).** Provides functional oversight to legal offices responsible for advising AF intelligence components. Responsible for IO training of judge advocates, civilian attorneys, and paralegals with intelligence activity responsibilities. In conjunction with SAF/GC, reviews intelligence related policy directives, regulations, and training policies. Voting member of the IO Panel.

2.6. **MAJCOMs, FOAs, and DRU Inspector General.**

2.6.1. Know what intelligence units and/or non-intelligence units that perform intelligence activities fall under your Commander's authorities and understand how the procedures of DoD 5240.1-R relate to their missions. (T-1)

2.6.2. Understand IG's responsibilities, as highlighted in DoD 5240.1-R, Procedures 14 and 15. (T-0)

2.6.3. Appoint, at a minimum, one primary and one alternate IO representative. (T-1)

2.6.4. Assess IO compliance of subordinate units IAW AFI 90-201. (T-1)

2.6.5. Ensure organizations that conduct intelligence activities have an established mechanism for reporting questionable activities. (T-1)

2.6.6. Report verified questionable intelligence activities and/or significant or highly sensitive matters, as required, to SAF/IG. (T-0)

2.6.7. Submit quarterly IO reports to SAF/IG. (T-0)

2.6.8. Complete initial IO training within 60 days of assignment/employment, annual refresher training, and any unit-specific training. (T-1)

2.7. **MAJCOMs, FOAs, and DRUs.**

2.7.1. Appoint, at a minimum, one primary and one alternate IO manager. (T-1)

2.7.2. Establish and manage IO programs that affect IO and ensure all personnel assigned or attached to their intelligence components receive IO training. (T-1)

2.7.3. Through their inspector general function, accomplish IO inspections required by AFI 90-201. **Note:** IO inspections of ANG intelligence units and staffs will normally be conducted by the gaining MAJCOM. However, they may also be inspected by the National Guard Bureau Inspector General when gaining MAJCOM inspection resources are insufficient or unavailable. (T-1)

2.7.4. Understand the responsibilities associated with intelligence oversight as outlined in DoD 5240.1-R. (T-0)

2.7.5. Understand the missions of subordinate organizations and those procedures of DoD 5240.1-R that relate to conducting those intelligence activities. (T-1)

2.7.6. Identify subordinate units with high-risk missions that increase opportunity of IO violations and ensure additional training is developed and implemented to mitigate added risk. (T-1)

2.7.7. Report verified questionable intelligence activities and/or significant or highly sensitive matters, as required, to the Inspector General IAW DoD 5240.1-R, Procedure 15. (T-0)

2.7.8. Must provide guidance to subordinate unit IO monitors on IO-related issues and concerns. (T-1)

2.7.9. Serves as approval authority and/or coordination manager for subordinate unit PUMs. (T-1)

2.7.10. Ensure completion of: initial IO training within 60 days of assignment or employment; annual refresher training; as well as any unit specific IO training. (T-1)

2.8. **Staff Judge Advocates/Legal Advisors responsible for units that perform intelligence activities.**

2.8.1. Know what intelligence units and/or non-intelligence units performing intelligence activities fall under your Commander's authorities. (T-1)

2.8.2. Understand the legal responsibilities as highlighted in DoD 5240.1-R, Procedures 14 and 15. (T-1)

2.8.3. Obtain the necessary clearances in order to provide legal advice on IO issues. (T-1)

2.8.4. Understand the missions of the organizations under your jurisdiction and the procedures of DoD 5240.1-R that relate to those missions. (T-1)

2.8.5. Complete initial IO training within 60 days of assignment or employment; annual refresher training; as well as any unit specific IO training. (T-1)

2.8.6. Report verified questionable intelligence activities and/or significant or highly sensitive matters, as required, to your organization's IG. (T-0)

2.9. **Commanders/Directors of units that perform intelligence activities.**

2.9.1. Appoint, at a minimum, one primary and one alternate IO monitor. (T-1)

2.9.2. Be familiar with IO responsibilities. (T-1)

2.9.3. Ensure that IO rules and regulations are followed by subordinate intelligence personnel and personnel performing intelligence functions. (T-0)

2.9.4. Determine when additional unit IO training is required to mitigate increased potential for IO incidents related to high-risk missions. (T-1)

2.9.5. As directed by AFIS, ensure IO program is inspected at least annually. (T-1)

2.9.6. At a minimum, designate primary and alternate IO monitors in writing. Additional IO monitors can be designated as appropriate to unit mission requirements. (T-2)

2.9.7. Ensure IO training, as required, is conducted. (T-1)

2.9.8. Complete: initial IO training within 60 days of assignment/employment; annual refresher training; as well as any unit specific training. (T-1)

2.10. **Intelligence Oversight Monitors.**

2.10.1. Ensure all personnel who conduct or supervise intelligence activities complete all required IO training. (T-1)

2.10.2. Ensure IO training records are maintained IAW AFI 36-2201. (T-1)

2.10.3. Ensure copies of Executive Order 12333, DoDD 5240.1, DoD 5240.1-R; DoDD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight;* and this instruction are available in hard or electronic copy. (T-1)

2.10.4. When required, develop additional unit IO training to mitigate increased potential for IO incidents related to high-risk missions. (T-1)

2.10.5. Ensure continual IO compliance by completing required program self-assessments. AF-assigned units will use the HAF IO Self-assessment checklist (SAC) available on MICT IAW the Commander's Inspection Program (CCIP). Units assigned to combat support agencies (i.e. National Security Agency (NSA)) or detailed to other organizations outside of the Department of the Air Force will comply with their assigned organization's respective inspection guidance. (T-1)

2.10.6. Provide assistance in rendering collectability determinations on information acquired about US persons within 90 days. IO monitors should utilize their operational chain of command if assistance is needed. (T-0)

2.10.7. For AF-assigned units, IO monitors will report verified questionable intelligence activities and/or significant/highly sensitive matters to their respective Wing Inspector General and MAJCOM IO managers. (T-0)

2.10.8. IO monitors assigned to combat support agencies or detailed to organizations outside the Department of the Air Force will report verified questionable intelligence activities and/or significant/highly sensitive matters IAW the assigned organization's reporting guidelines and up channel to their respective Wing IG and MAJCOM IO manager. (T-1)

2.11. **Intelligence Personnel.**

2.11.1. Must know the mission of your organization and the responsibilities in regards to IO. (T-1)

2.11.2. Must know your organization's IO monitors. (T-1)

2.11.3. Must be familiar with DoD 5240.1-R, Procedures 1-4, 14 and 15, this instruction, and any organization-specific instructions concerning IO. (T-1)

2.11.4. Complete initial IO training within 60 days of assignment/employment and maintain annual currency. Currency should be maintained during deployments, extended temporary duty assignments (TDYs). (T-1)

2.11.5. Assigned to AF-subordinate units will report verified questionable intelligence activities and/or significant or highly sensitive matters to their respective AF IO monitor. (T-0)

2.11.6. Assigned to a Combat Support Agency or detailed to organizations outside the Department of the Air Force will report verified questionable intelligence activities and/or significant or highly sensitive matters IAW the assigned organization's reporting guidelines and up channel to their respective AF IO monitor. (T-1)

**3. Training.**

3.1. All personnel assigned to units that perform or support intelligence activities must complete IO training. (T-1)

3.1.1. Completion of the standardized IO CBT module hosted on Advanced Distributed Learning Service (ADLS) is the designated course for AF personnel supporting

intelligence activities. Requests for alternate IO training must be submitted to the MAJCOM IO Manager and approved by the AF/A2 IO manager. AF intelligence members detailed to organizations outside of the AF (i.e. National Geospatial-Intelligence Agency (NGA), NSA) who complete local IO training may substitute such training, as long as it has been approved by the AF/A2 IO manager. Alternate training approval will be documented via memorandum for record (MFR) and maintained by the AF/A2 IO manager. Approved alternate IO training must be reviewed annually to ensure that it continues to meet AF requirements. (T-1)

3.1.2. AF Unit Training Managers (UTM) monitor all AF and non-AF IO training completion. Personnel are responsible for providing proof of non-ADLS IO training to UTMs since external training cannot be automatically tracked via ADLS. It is the member's responsibility to maintain IO training currency. Deployed members will ensure they remain current through the duration of the deployment. (T-1)

3.1.3. Annual IO training is a minimum requirement. Commanders are encouraged to develop additional training as necessary to meet unique unit mission requirements. (T-1)

3.2. **Initial Training.** IO monitors will ensure all AF personnel and other personnel, who are assigned or attached to, or employed by, AF intelligence components complete initial IO training through ADLS. AF personnel assigned to organizations outside the Department of the Air Force will also complete AF IO training via ADLS, unless training substitutions are authorized. IO monitors will ensure all intelligence personnel complete appropriate IO training within 60 days (NLT 180 days for AFRC/ANG units and assigned or attached Individual Mobilization Augmentees) of assignment. IO monitors will also ensure all staff judge advocates and inspectors general complete IO training within 60 days of employment or assignment. (T-1)

3.3. **Annual Training.** IO monitors will ensure all personnel, who are assigned to, attached to, or employed by, AF intelligence components complete annual training through ADLS. AF personnel who have been authorized training substitutions are required to complete formal IO training on an annual basis, regardless of the assigned organization's periodic training requirements. UTMs will utilize the ADLS system to maintain records of personnel IO training or locally produced training trackers when conducting additional training requirements. (T-1)

3.4. **Mission-Specific Training.** Due to unique intelligence missions or specific operational requirements, some intelligence personnel may require additional IO training. For example, units that conduct collection missions or units responsible for intelligence dissemination are at a higher risk of IO violations. MAJCOMS or unit commanders will determine if their units have high-risk missions that may increase opportunity for IO violations. If determined to be high-risk, unit commanders may mandate additional IO training for unit personnel. Mission-specific training is supplemental and does not exempt personnel from completing their respective annual IO training. (T-1)

**4. Program Inspection Guidance.** AF IO inspection guidance is governed by AFI 90-201. IAW with AFI 90-201, the IO program can be divided into three inspection groups: Unit, IG, ATSD (IO).

4.1. **Unit Inspections.** Unit Inspections are conducted at the Wing level on a subordinate agency or as part of the CCIP. Commanders are responsible for ensuring compliance within their units and inspection frequency within the unit. Wing IG will validate and verify SAC responses. (T-1)

4.2. **Air Force Inspector General Inspections.** The Wing IG will ensure that unit IO programs are assessed annually (by the Wing/IG team, or by the MAJCOM/IG team) IAW commander guidance and AFI 90-201. Additionally, the IO program will be externally assessed during the 2-year Unit Effectiveness Inspection period. (T-1)

4.3. **ATSD (IO) Inspections.** The ATSD (IO) conducts independent inspections of DoD Intelligence activities worldwide, ranging from intelligence staffs at strategic headquarters to tactical intelligence activities in the field. These inspections are independent of CCIP and IG inspection programs and can occur at any time. Inspected units will be notified prior to ATSD (IO) inspections.

**5. Identifying, Investigating and Reporting Questionable Activities.**

5.1. **Identifying and Investigating Questionable Activities.** Commanders will report any questionable activity and investigate to the extent necessary to determine whether the reported activity violates law, executive order, Presidential directive, or DoD directive or policy. Officials responsible for investigations may obtain additional assistance from within the component concerned or from other DoD components, when necessary, to complete investigations in a timely manner. Investigations will be conducted as quickly as possible. Violations should not be considered a "questionable activity" in this unless there is some nexus between the activity and an intelligence function. SAF/GC, in coordination with the servicing legal office or higher legal office, will provide assistance in verifying Questionable Intelligence Activities and Highly Sensitive Matters. (T-0)

5.2. **Reporting Questionable Activities and Highly Sensitive Matters.** AF agencies, units and personnel must report any questionable activity IAW DoD 5240.1-R, Procedure 15 to SAF/GC and their servicing or higher legal office. (T-0) Once a questionable activity or a highly sensitive matter has been investigated by SAF/IG and verified by legal officials or the JA chain, the matters must be reported immediately. DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities Significant or Highly Sensitive Matters*, Attachment 2, provides reporting parameters and submission procedures. These reports must be filed immediately. (T-0)

5.2.1. SAF/IG, SAF/GC, and AF/A2 will immediately report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters, as required, to the Attorney General, the DoD General Counsel and the ATSD(IO). (T-0) Any such reports are exempt from Report Control Symbol (RCS) licensing procedures according to AFI 33-324, *The Air Force Information Collections and Reports Management Program.* (T-1)

5.2.2. MAJCOMs/FOAs/DRUs similarly will report verified Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters and crimes to SAF/IG through their Inspectors General, providing information copies of the report to SAF/GC and AF/A2. (T-1)

5.2.3. Air Force agencies, units, and personnel must report verified Questionable Activities and/or Significant or Highly Sensitive Matters, and crimes to SAF/GC, SAF/IG, AF/JA, AF/A2, the DoD General Counsel or ATSD(IO) using the supervisory chain of command when feasible. (T-0) Such reports will be expeditiously provided to the inspector general at the first level at which an Inspector General is assigned and not associated with the questionable activity, with copies to the Staff Judge Advocate and, unless the Inspector General determines such reporting would not be appropriate, to senior intelligence officers at the same level. (T-1) This report must be made regardless of whether a criminal or other investigation has been initiated. (T-1) Units assigned or detailed to non-AF organizations will follow the assigned or detailed organization's for reporting Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters. (T-1) If no procedures exist for the assigned or detailed organization, AF units will report Questionable Intelligence Activities and/or Significant or Highly Sensitive Matters to their Inspector General. (T-1)

5.3. **Submitting Quarterly IO Reports.** Each MAJCOM, FOA, or DRU Inspector General responsible for an AF organization or staff subject to this instruction must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI two calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a single AF report, coordinate with SAF/IG, SAF/GC, AF/JA and AF/A2, and provide to ATSD(IO). Inputs must include: (T-1)

5.3.1. A description of each new verified questionable intelligence activity or significant or highly sensitive matter identified during the quarter. (T-1)

5.3.2. Any updates to previously reported verified questionable intelligence activities or significant or highly sensitive matters. (T-1)

5.3.3. A description of corrective actions taken regarding questionable intelligence activities or significant or highly sensitive matters. (T-0)

5.3.4. A list of completed IO evaluations or inspections by unit and location and a summary of the results or trends. Include any questionable intelligence activities or significant or highly sensitive matters discovered during the inspection, the familiarity of personnel with IO requirements, and the adequacy of organization IO programs, structure, and processes. If any evaluations or inspections reveal deficiencies, note the corrective action taken. (T-1)

5.3.5. Significant oversight activities undertaken during the quarter and any suggestions to improve the IO program. (T-1)

5.3.6. The MAJCOM, FOA or DRU report will also include a list of the units and staffs for which they have IO and inspection requirements (specifying MAJCOM, parent organization, unit designation, and location). **Note:** This list may be classified due to the specific unit's mission. Ensure classified packages follow proper classification guidelines IAW DoD 5200.01, Volume 1, *Information Security Program: Overview, Classification, and Declassification*, AFI 31-401, *Information Security Program Management*, DoDM 5105.21, Volume 1, *Department of Defense Sensitive Compartmented Information (SCI) Administrative Security Manual, Administration of Information and Information Systems Security*, and Intelligence Community Directive 710, *Classification and Control Markings System*. (T-1)

**6. DOMESTIC IMAGERY.** AF components may, at times, require newly collected or archived domestic imagery to perform certain missions. Domestic imagery is defined as any imagery collected by satellite (national or commercial) and airborne platforms that cover the land areas of the 50 United States, the District of Columbia, and the territories and possessions of the US, to a 12 nautical mile seaward limit of these land areas.

6.1. **Collecting information on specific targets inside the US raises policy and legal concerns that require careful consideration, analysis, and coordination with legal counsel.** Therefore, AF components should use domestic imagery only when there is a justifiable need to do so, and then only IAW EO 12333; the National Security Act of 1947, as amended; DoD 5240.1-R; and this instruction. The following generally constitute legally valid requirements for domestic imagery (Note: A legally valid requirement does not preclude unit requirement to obtain PUM when mandated by MAJCOM or higher authority.):

6.1.1. Natural Disasters. Locations in support of government planning for, emergency response to, or recovery from events such as tornadoes, hurricanes, floods, mudslides, fires, and other natural disasters.

6.1.2. Counterintelligence, Force Protection, and Security-related Vulnerability Assessments. Requirements in support of critical infrastructure analysis on federal or private property where consent has been obtained as appropriate.

6.1.3. Environmental Studies. Requirements in support of studies of wildlife, geologic features, or forestation, or similar scientific, agricultural, or environmental studies not related to regulatory or law enforcement actions.

6.1.4. Exercise, Training, Testing, or Navigational Purposes. Requirements in support of system or satellite calibration, sensor evaluation, algorithm or analytical developments and training or weapon systems development or training.

6.2. **Domestic Imagery from Satellites.**

6.2.1. National Satellites. The NGA is responsible for the legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites. AF components must follow policy and procedures established in the National System for Geospatial Intelligence Manuals (NSGM) FA 1806 Revision 5, *Domestic Imagery*. AF components must submit a PUM signed by the organization's certifying government official each year to NGA. The PUM must define the requirements for domestic imagery, outline its intended use, and include a proper use statement acknowledging awareness of legal and policy restrictions regarding domestic imagery. NGA will review the PUM to ensure it constitutes a legally valid requirement for domestic imagery. AF components must submit a Domestic Imagery Request (DIRs) to NGA for any ad hoc domestic imagery requirements that fall outside the scope of an approved PUM. (T-0)

6.2.2. Commercial Satellites. Domestic imagery from commercial systems does not fall under the authorities of the Director of National Intelligence, and therefore the use of domestic commercial imagery will be dependent upon the authorities and the responsibilities of each user organization. For guidance regarding whether or not a PUM is required, users must reference the NSGM FA 1806. If no PUM is required, AF units must maintain an internal MFR describing the purpose of the domestic imagery and the unit official approving the use. At a minimum, approval authority for MFRs will be the

unit commander and MFRs will be reviewed on a no less than annual basis while they remain applicable. If obtained imagery specifically identifies a US person (include private property), then the rules and procedures contained in DoD 5240-1.R, in particular those regarding retention, must be followed. AF intelligence units must not conduct or give the appearance of conducting collection, exploitation or dissemination of commercial imagery or imagery associated products for other than approved mission purposes. (T-1)

6.3. **Domestic Imagery from AF Platforms.** An approved PUM must be on file with the appropriate Combatant Command, per their procedures, or with the appropriate AF MAJCOM or FOA (or delegated/designated sub-component PUM authority) before airborne, tactical DoD satellite platforms, or ground platforms can be tasked to collect domestic imagery. Note that Tactical Satellites are considered "airborne" platforms and so PUM approval authority does not reside with NGA. Approval for PUM requests is hereby delegated to MAJCOM and FOA commanders. Legal review at MAJCOM/FOA level is required before approval and reviews should be filed with the approved PUM requests. In the event of an emergency or crisis where US Northern Command (USNORTHCOM) is designated as lead DoD Operational Authority, all related requests for domestic imagery from airborne or tactical DoD satellite platforms must be coordinated with USNORTHCOM to ensure compliance with proper use provisions. AF components must submit a PUM request through the MAJCOM to the designated approval authority for any ad hoc DIR. These PUMs must be IAW the format instructions found in Attachment 2. (T-1)

6.4. **Distribution of Domestic Imagery.** Distribution of domestic imagery to parties other than those identified in the approved PUM, DIR, or MFR is prohibited, unless the recipient is reasonably perceived to have a specific, lawful governmental function requiring it IAW dissemination guidelines. Unless otherwise approved, domestic imagery must be withheld from all general access database systems (e.g., Intelink). (T-1)

6.5. **Navigational/Target Training activities.**

6.5.1. AF units with weapon system video and tactical ISR capabilities may collect imagery during formal and continuation training missions as long as the collected imagery is not for the purpose of obtaining information about specific US persons or private property. Collected imagery may incidentally include US persons or private property without consent. Imagery may not be collected for the purpose of gathering any specific information about a US person or private entity without consent. Any stored imagery will not be retrievable by reference to US person identifiers. (T-1)

6.5.2. Remotely Piloted Aircraft (RPA) activities are highly scrutinized and often require higher level approvals to operate. RPAs will not operate outside of DoD Special Use Airspace without MAJCOM or higher level approval and will not image outside of DoD airspace without specific authorization. (T-0)

6.5.3. AF Remotely Piloted Aircraft (RPA) operations, exercise and training missions will not conduct nonconsensual surveillance on specifically identified US persons, unless expressly approved by the Secretary of Defense, consistent with US law and regulations. Civil law enforcement agencies, such as the US Customs and Border Patrol, Federal Bureau of Investigations (FBI), US Immigration and Customs Enforcement, and the US Coast Guard, will control any such data collected. (T-0)

**7. Force Protection.**

7.1. **Intelligence Support to Force Protection.** AFI 14-119, *Intelligence Support to Force Protection (FP)*, stipulates that intelligence personnel at all levels will work in coordination with their cross-functional counterparts (e.g., AFOSI, SF, ATOs, etc.) to ensure FP threat/intelligence requirements are satisfied. If during the course of routine, non-force protection related, intelligence activities and authorized missions, AF intelligence components receive information identifying US persons as an alleged threat to DoD or civilian individuals, entities or structures, such threats should be reported IAW the rules governing reporting of incidentally acquired threat information. (T-1)

7.2. **AF Intelligence Assets Assigned to FP mission.** AF intelligence assets assigned a mission to support force protection activities by a governmental entity that has responsibility for countering the threat may assist in fusing law enforcement and counterintelligence, with intelligence information in support of force protection (e.g., antiterrorism and/or law enforcement activities), consistent with IO procedures. AFI 14-119 provides guidance to support force protection mission execution.

**8. Procedural Guidance.** AF intelligence components may only engage in activities involving the deliberate collection of information about US persons under the procedures set forth in DoD 5240.1-R, AFI 71-101V4, *Counterintelligence* and this instruction. (T-0)

8.1. **General.** Any collection, retention and/or dissemination of US person information must be based on a proper function/mission assigned to the component and must follow the guidance in DoD 5240.1-R, AFI 71-101V4 and this instruction. (T-0)

8.2. **Collection.** Information about US persons may be collected if it falls within one or more of the thirteen categories of information specified in DoD 5240.1-R, Procedure 2. (T-0)

8.2.1. Temporary Retention. Information inadvertently received about US persons may be kept temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be collected under the provisions of Procedure 2, DoD 5240.1-R and permanently retained under the provisions of Procedure 3, DoD 5240.1-R. If there is any doubt as to whether the US person information may be collected and permanently retained, the receiving unit should seek advice through the chain of command, Staff Judge Advocate, or IO monitor. The unit/MAJCOM IO Monitor must provide assistance in rendering collectability determinations. When appropriate, assistance may be requested from AF/A2. A determination on whether information is collectible must be made within 90 days. (T-0)

8.2.1.1. If a determination is made that information is not properly collectible before the expiration of the 90 day period, it must be purged or transferred immediately. (T-0)

8.2.1.2. Even though information may not be collectible, it may be retained for the length of time necessary to transfer it to another DoD entity or government agency to whose function it pertains.

8.2.2. Means of Collection. When AF intelligence components are authorized to collect information about US persons, they may do so by any lawful means, subject to the following limitations.

8.2.2.1. Least Intrusive Means. Collection of information about US persons shall be accomplished by the least intrusive means. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought. (T-0)

8.2.2.2. Foreign Intelligence Collection within the United States. Within the US, foreign intelligence concerning United States persons may be collected only by overt means except as provided below. Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that the information is being provided to the DoD, or a component thereof:

8.2.2.2.1. The foreign intelligence sought must be significant and not collected for the purpose of acquiring information concerning the domestic activities of any US person; (T-0)

8.2.2.2.2. The foreign intelligence cannot reasonably be obtained by overt means;

8.2.2.2.3. The collection of such foreign intelligence has been coordinated with the FBI;

8.2.2.2.4. The Secretary of the Air Force has approved the use of other than overt means and has delegated the authority to approve such action to AF/A2. AF/A2. AF/A2 will provide a copy of any such approval to the Undersecretary of Defense for Intelligence.

8.3. **Retention.** Retention limitations apply to information about US persons that is knowingly retained without the consent of the person whom the information concerns. These limitations do not apply to information retained solely for administrative purposes or is required by law to be maintained. "Retention" refers only to the maintenance of information about US persons that can be retrieved by reference to the person's name or other identifying data. Any US person information that is properly collected and retained will be reviewed periodically to ensure that continued retention serves the purpose for which it was collected and stored, and that retention remains necessary to the conduct of authorized functions of the AF intelligence component concerned. (T-0)

8.4. **Dissemination.** US person information in the possession of an AF intelligence component may be disseminated pursuant to law, a court order, or IAW the following criteria:

8.4.1. The information was properly collected or retained or both under Procedures 2 and 3 of DoD 5240.1-R.

8.4.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function and is:

8.4.2.1. An employee of the DoD or an employee of a contractor of the DoD who has a need for such information in the course of their official duties.

8.4.2.2. A law enforcement entity of federal, state or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce.

8.4.2.3. An agency within the intelligence community. Whether the information is relevant to the responsibilities of any such intelligence agency is a determination to be made by the agency concerned.

8.4.2.4. An agency of the federal government authorized to receive such information in their performance of a lawful governmental function.

8.4.2.5. A foreign government and dissemination is undertaken pursuant to an agreement or other understanding with such government.

8.5. **Electronic Surveillance.**

8.5.1. Electronic surveillance, for counterintelligence purposes must be conducted IAW instructions and procedures promulgated by the Commander, AFOSI, approved by the Secretary of the Air Force, and contained in AFI 71-101 V4. (T-0)

8.5.2. Electronic Surveillance targeting U.S. persons and non U.S. persons in and outside the U.S. for counterintelligence purposes will be conducted and approved IAW DoD 5240.1-R and AFI 71-101V4. (T-0)

8.5.3. Requests to perform electronic surveillance, to include computer network exploitation, for foreign intelligence collection or against US persons abroad for foreign intelligence purposes, whether consensual or nonconsensual, must be forwarded to the AF/A2 for approval. AF/A2 will coordinate with SAF/GCI. (T-0)

8.6. **Concealed Monitoring.** Monitoring of individuals within the US or US persons outside the United States, where the subject of such monitoring does not have a reasonable expectation of privacy and no warrant would be required if the monitoring were undertaken for law enforcement purposes, requires the approval of the Commander, AFOSI after consultation with AFOSI/JA (for counterintelligence) or the AF/A2 after consultation with SAF/GCI (for foreign intelligence).

8.6.1. Approval officials must determine that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions and does not constitute electronic surveillance. (T-0)

8.6.2. Within the US, an AF intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by DoD or otherwise in the course of an investigation conducted for counterintelligence purposes pursuant to the *Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation,* dated 5 April 1979.

8.6.3. Outside the US, concealed monitoring may be conducted on installations and facilities owned, or otherwise lawfully occupied by the DoD. Monitoring outside such facilities shall only be conducted after coordination with appropriate host country officials, if such coordination is required by the governing status of forces agreement (SOFA), and with the Central Intelligence Agency (CIA). (T-0)

8.7. **Physical Searches.** A physical search is any intrusion upon a person or a person's property or possessions to obtain items of property or information. Examination of areas that are in plain view and visible to the naked eye if no physical trespass is required, or of items that are abandoned in a public place, does not constitute a physical search. Any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to DoDD 5240.1, Procedure 5, Parts 1 and 2, does not constitute a physical search.

8.7.1. Physical Searches within the United States. AFOSI is authorized to conduct nonconsensual searches in the US for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military judge or magistrate, or a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers. AF intelligence components may not conduct nonconsensual physical searches within the US for foreign intelligence or counterintelligence purposes.

8.7.2. Physical Searches outside the United States.

8.7.2.1. AFOSI may conduct nonconsensual physical searches for counterintelligence purposes of persons or property of active duty military personnel outside the US when authorized by a military judge or magistrate, or a commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe such persons are acting as agents of foreign powers.

8.7.2.2. For foreign intelligence or counterintelligence purposes, other non-consensual physical searches of the person or property of US persons, may be conducted only pursuant to the approval of the Attorney General or higher level as required.

8.7.2.3. Within a commander's SOFA authorities, nonconsensual physical searches of non-US persons abroad must be IAW any applicable SOFA and approved by the Installation Commander. Nonconsensual physical searches of non-US persons abroad may be approved by the Commander, AFOSI for counterintelligence purposes and by the AF/A2 for foreign intelligence purposes. (T-1)

8.8. **Searches and Examination of Mail.**

8.8.1. Applicable postal regulations do not permit the AF to detain or open first class mail within US postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service. Searches of first class mail in US military postal channels overseas may only be authorized under procedures established in DoD 4525.6-M, *Department of Defense Postal Manual*, Chapter 10.

8.8.2. AF intelligence components may request that appropriate US postal authorities inspect, or authorize the inspection of second, third or fourth class mail in US postal

channels IAW applicable postal regulations. Such components may also request that US postal authorities detain, or permit detention of, mail that may become subject to search under applicable postal regulations.

8.8.3. AF intelligence components may open mail to or from a US person that is found outside US postal channels only with the approval of the Attorney General. Any requests for such authorization for foreign intelligence purposes will be forwarded through the AF/A2, and for counterintelligence purposes through the Commander, AFOSI. (T-1)

8.8.4. Mail outside US postal channels when both the sender and intended recipient are other than US persons, may be searched if such search is otherwise lawful and consistent with any applicable SOFA. For counterintelligence purposes, such searches must be approved by the Commander, AFOSI, and for foreign intelligence purposes, by the AF/A2. (T-1)

8.8.5. Mail Covers. The Commander, AFOSI may request US postal authorities examine mail in US postal channels for counterintelligence purposes, IAW postal regulations. The Commander, AFOSI may also request mail covers from appropriate foreign officials, with respect to mail to or from a US person that is outside US postal channels, IAW appropriate law and procedures of the host government and any SOFA that may be in effect.

8.9. **Physical Surveillance.** Physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. Any physical surveillance that occurs outside a DoD installation shall be coordinated with the FBI (within the US), CIA (outside the US), or other agency as appropriate. (T-0)

8.9.1. Physical surveillance for counterintelligence purposes, both within and outside the US, shall be approved and conducted IAW DoD 5240.1-R, AFI 71-101V4 and procedures established by the Commander, AFOSI. (T-0)

8.9.2. Physical surveillance for foreign intelligence purposes shall be approved and conducted IAW DoD 5240.1-R and procedures established by the AF/A2, or his/her designee. (T-0)

8.10. **Undisclosed Participation in Organizations.** Undisclosed participation that occurs outside a DoD installation must be coordinated with the FBI (within the US), through the AFOSI, CIA (outside the US), or other agency as required. Intelligence component employees do not require permission to participate in organizations for solely personal purposes. Participation by an employee of an AF intelligence component, on behalf of an intelligence component, in any organization within the US or any organization outside the US that constitutes a US person, must be approved IAW the requirements in subparagraphs below. (T-0)

8.10.1. Undisclosed participation, for counterintelligence purposes, must be approved and conducted IAW procedures approved by the Commander, AFOSI, and, DoD 5240.1-R. (T-0)

8.10.2. Undisclosed participation by personnel assigned to AF ISR Agency for foreign intelligence purposes must be approved by the AF ISR Agency Commander (or his designee) and such participation must be conducted IAW DoD 5240.1-R. (T-0)

8.10.3. Outside AF ISR Agency, undisclosed participation for foreign intelligence purposes must be approved by AF/A2, or its delegate, and IAW DoD 5240.1-R and procedures established by AF/A2. (T-0)

8.11. **Contracting for Goods and Services.** DoD 5240.1-R, Procedure 11 applies to contracting or other arrangements with academic institutions, commercial organizations, private institutions, or private individuals within the United States for the procurement of goods and services by or for an AF intelligence component. It does not apply to contracting with government entities, or to the enrollment of individual intelligence personnel as students with academic institutions. When non-disclosure of intelligence component sponsorship is necessary in contracts for enrollment of students in academic institutions, the provisions related to undisclosed participation in organizations apply. Air Force intelligence components may contract with Commercial Organizations, Private Institutions, and Individuals within the US without revealing the sponsorship of the intelligence component only if the following apply:

8.11.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, incident to approved activities; or

8.11.2. There is a written determination by the Secretary or Under Secretary of the Air Force that the sponsorship by an AF intelligence component must be concealed to protect the activities of the intelligence component concerned. This authority may not be delegated. (T-0)

8.12. **Assistance to Law Enforcement.**

8.12.1. Cooperation with law enforcement authorities. Subject to the limitations detailed in DoD 5240.1-R, AF intelligence components may cooperate with law enforcement authorities IAW DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, for the purpose of:

8.12.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

8.12.1.2. Protecting DoD employees, information, property and facilities;

8.12.1.3. Preventing, detecting, or investigating other violations of law.

8.12.2. Types of permissible assistance. AF intelligence components may only provide the types of assistance to law enforcement authorities delineated above. Assistance may not be provided for, or participation in, activities that would not be permitted under this instruction.

8.12.2.1. Violations of US federal law. Incidentally acquired information reasonably believed to indicate a violation of federal law must be provided to appropriate federal law enforcement officials through AFOSI channels. (T-1)

8.12.2.2. Other violations of law. Information incidentally acquired during the course of AF counterintelligence activities reasonably believed to indicate a violation of state, local, or foreign law will be provided to appropriate officials IAW procedures established by the Commander, AFOSI. Information incidentally acquired during the course of AF foreign intelligence activities reasonably believed to indicate a violation of state, local, or foreign law will, unless otherwise decided by AF/A2 for national security reasons, be provided to AFOSI IAW procedures established by the AF/A2, or his/her designee, for investigation or referral to the appropriate law enforcement agency. Information covered by this paragraph includes US person information. (T-1)

8.12.2.3. Provision of specialized equipment and facilities. Specialized intelligence equipment and facilities may be provided to federal law enforcement authorities; and, when lives are endangered, to state and local law enforcement authorities, only with the approval of the SecAF delegated authority and the concurrence of SAF/GC.

8.12.2.4. Assistance of AF intelligence personnel. AF intelligence personnel may be assigned to assist federal law enforcement authorities with the approval of the SecAF delegated authority and the concurrence of SAF/GC. Under certain exigent circumstances (e.g., when lives are in danger), AF intelligence personnel may be assigned to assist state and local law enforcement authorities, provided such assistance has been approved by the Deputy Chief for Manpower, Personnel, and Services (AF/A1) and SAF/GC.

8.13. **Experimentation on Human Subjects for Intelligence Purposes.** AF intelligence components do not engage in experimentation involving human subjects for intelligence purposes. Any exception would require approval by the Secretary or Under Secretary of the Air Force and would be undertaken only with the informed consent of the subject and IAW procedures established by AF/SG to safeguard the welfare of subjects.

8.13.1. Experimentation means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

8.13.2. Experimentation is conducted on behalf of an AF intelligence component if it is conducted under contract to AF or to another DoD component for the benefit of the AF or at the request of the AF regardless of the existence of a contractual relationship.

8.13.3. For purposes of this instruction, the term “human subjects” includes any person, whether or not such person is a US person. No prisoners of war, civilian internees, retained, and detained personnel as covered under the Geneva Conventions of 1949 may be the subjects of human experimentation.

**9. Reporting of Incidentally Acquired Threat Information.** During the course of routine activities and authorized missions, AF intelligence components may receive information (including information identifying US persons) regarding potential threats to life or property (whether DoD personnel, installations or activities, or civilian lives or property). Any such information must be passed to appropriate authorities. (T-0)

9.1. If such threat information involves an imminent threat to life or risk of serious property damage, the AF intelligence component must immediately notify appropriate entities with responsibility for countering the threat (e.g., Base Command Section, Security Forces, FBI, Municipal Police Department, etc.). The AF intelligence component must also immediately notify AFOSI. In the event immediate notification of the local AFOSI unit is not possible, the AF intelligence component will notify the AFOSI Global Watch Center, Commercial (571) 305-8484 and DSN (312) 240-8484, or Commercial Toll Free 1-877-246-1453. (T-1)

9.2. In the absence of an imminent threat, AF intelligence components will limit notification to AFOSI who will determine whether further reporting will unacceptably compromise potential investigative or operational activities and forward to other authorities as appropriate. (T-1)

9.3. Threat information may only be withheld from dissemination upon the approval of AF/A2 for foreign intelligence or Commander, AFOSI for counterintelligence, and only for national security reasons.

**10. The Internet.** While much of the information posted on the Internet is publicly available, AF intelligence components must have an official tasked mission before collecting, retaining, or disseminating publicly available information about US persons. Certain internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation. This also applies to information found on Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communication System (JWICS). (T-1)

ROBERT P. OTTO, Lt Gen, USAF
Deputy Chief of Staff, Intelligence
Surveillance and Reconnaissance

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, 2 April 2004

AFI 14-119, *Intelligence Support to Force Protection (FP),* 4 May 2012

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

AFI 33-324, *The Air Force Information Collections and Reports Management Program*, 6 March 2013

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFI 71-101 Volume 1, *Criminal Investigations*, 8 April 2011

AFI 71-101 Volume 4, *Criminal Investigations*, 8 November 2011

AFI 90-201, *Counterintelligence,* 2 August 2013

AFMAN 33-363, *Management of Records,* 1 March 2008

Executive Order Number 12333, *United States Intelligence Activities*, December 4, 1981

National Security Act of 1947, 50 United States Code, Sections 401 et sequentia

DoDD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))*, April 24, 2013

DoDD 5240.1, *DoD Intelligence Activities*, August 27, 2007

DoDD 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials*, January 15, 1986

DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, February 27, 2013

DTM 08-052 – *DoD Guidance for Reporting Questionable Intelligence Activities Significant or Highly Sensitive Matters,* June 17, 2009

DoD 4525.6-M, *Department of Defense Postal Manual,* August 15, 2002

DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,* December 1, 1982

DoDM 5105.21, Volume 1, *Department of Defense Sensitive Compartmented Information (SCI) Administrative Security Manual, Administration of Information and Information Systems Security,* October 19, 2012

DoD 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, February 24, 2012

United States Signals Intelligence Directive (USSID) SP0018, 25 January 2011

National System for Geospatial Intelligence Manual FA 1806, *Domestic Imagery*, Revision 5, March 2009

*Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation,* 5 April 1979

Intelligence Community Directive 710, *Classification and Control Markings System,* 21 June 2013

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication,* 22 September 2009

***Abbreviations and Acronyms***

**ADLS**—Advance Distributed Learning Service

**AF/A1**—Deputy Chief of Staff for Manpower, Personnel and Services

**AF/A2**—Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance

**AFI**—Air Force Instruction

**AF ISR Agency**—Air Force Intelligence, Surveillance, and Reconnaissance Agency

**AFOSI**—Air Force Office of Special Investigations

**AFPD**—Air Force Policy Directive

**AFRC**—Air Force Reserve Command

**AF/SG**—Surgeon General

**ANG**—Air National Guard

**ATSD(IO)**—Assistant to the Secretary of Defense for Intelligence Oversight

**CBP**—United States Customs and Border Patrol

**CBT**—Computer Based Training

**CCIP**—Commander's Inspection Program

**CIA**—Central Intelligence Agency

**CoP**—Community of Practice

**DIR**—Domestic Imagery Request

**DoD**—Department of Defense

**DoDD**—Department of Defense Directive

**DRU**—Direct Reporting Unit

**EO**—Executive Order

**FBI**—Federal Bureau of Investigation

**FOA**—Field Operating Agency

**IAW**—In Accordance With

**IG**—Inspector General

**IO**—Intelligence Oversight

**ISR**—Intelligence, Surveillance, and Reconnaissance

**JA**—Judge Advocate

**JAG**—Judge Advocate General

**JWICS**—Joint Worldwide Intelligence Communication System

**MAJCOM**—Major Command

**MFR**—Memorandum For Record

**NGA**—National Geospatial-Intelligence Agency

**NSA**—National Security Agency

**OPR**—Office Of Primary Responsibility

**PUM**—Proper Use Memorandum

**USD(I)**—Undersecretary of Defense for Intelligence

**USNORTHCOM**—United States Northern Command

**RDS**—Records Disposition Schedule

**SAF/GC**—Secretary of the Air Force General Counsel

**SAF/IG**—Secretary of the Air Force Inspector General

**SCI**—Sensitive Compartmented Information

**SIGINT**—Signals Intelligence

**SIPRNET**—Secret Internet Protocol Router Network

**SOFA**—Status of Forces Agreement

**T-0**—Tier 0

**T-1**—Tier 1

**T-2**—Tier 2

**T-3**—Tier 3

**TDY**—Temporary Duty

**US**—United States

**USSID**—United States Signals Intelligence Directive

**UTM**—Unit Training Monitor

***Terms***

**Air Force Intelligence Component**—All personnel and activities of the organization of the AF Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, counterintelligence units of the Air Force Office of Special Investigations, Air Force Intelligence Analysis Agency, and other organizations, staffs, and offices when used for foreign intelligence or counterintelligence activities to which EO 12333 (part 2) applies.

**Certifying Government Official**—A U.S. Government employee in authority over the requesting individual (i.e., branch chief, chief of collections, requesting military organization, etc.) who will verify and remain accountable for the accuracy of the request. The official will ensure that the requested imagery and products derived from domestic imagery are maintained subject to this policy and all other pertinent security controls.

**Computer Network Exploitation**—Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE *and network exploitation (Net-E)*."

**Counterintelligence**—Information gathered and activities conducted to prevent espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

**Domestic Imagery Request (DIR)**—The request for collection, processing, dissemination, exploitation, briefing, or publication of domestic imagery when that need falls outside the scope of an approved PUM and is not a reflection of a change in an organization's mission. Generally reflects ad hoc requirements for domestic imagery.

**Electronic Surveillance**—Electronic surveillance, as defined at 50 USC 1801(f)(1)-(4), and as conducted by DoD intelligence components targeting US Persons to collect foreign intelligence information under circumstances in which a warrant would be required for law enforcement purposes. Note that this includes, per 50 USC 1801(f)(4), the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication (such as oral communications acquired by hidden microphone, or location information revealed through the use of a transponder or tracker device), under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

**Experimentation**—Any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.

**Foreign Intelligence**—Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

**Human Subjects**—Any person, whether or not such person is a US person. No prisoners of war, civilian internees, retained, and detained personnel as covered under the Geneva Conventions of 1949 may be the subjects of human experimentation.

**Intelligence Activities**—Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333. Note that EO 12333 assigns the Services' intelligence components responsibility for: 1, "Collection, production, dissemination of military and military related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking;" and 2, "Monitoring of the development, procurement and management of tactical intelligence systems and equipment and conducting related research, development, and test and evaluation activities."

**Non-United States Person**—A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person. A person or organization outside the United States is presumed not to be a US person, unless specific information to the contrary is obtained. An alien in the United States is presumed not to be a US person, unless specific information to the contrary is obtained.

**Organization**—Includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis.

**Overt**—Methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that the information is being provided to the DoD, or a component thereof.

**Physical Surveillance**—A systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person who is neither a party thereto nor visibly present thereat, through any means not involving electronic surveillance.

**Proper Use Memorandum (PUM)**—A memorandum signed annually by an organization's Certifying Government Official. The imagery user organization will submit this memorandum annually. It defines their requirements and intended use, and contains a proper use statement that acknowledges their awareness of the legal and policy restrictions regarding domestic imagery.

**Questionable Activity**—Any intelligence activity, as defined in Executive Order 12333 (Reference (f)), that may be unlawful or contrary to Executive Order, Presidential directive, or applicable DoD policy governing that activity.

**Retention**—The maintenance of information about US persons that can be retrieved by reference to the person's name or other identifying data.

**Significant or Highly Sensitive Matters**—A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity: (1) Involving congressional inquiries or investigations, (2) That may result in adverse media coverage, (3) That may impact on foreign relations or foreign powers, or (4) Related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations.

**Tier 0 (T-0)**—Determined by respective non-AF authority (e.g., Congress, White House, OSD, JS). The requirement is external to AF. Requests for waivers must be processed through command channels to publication OPR for consideration. (AFI 33-360)

**Tier 1 (T-1)**—Non-compliance puts Airmen, commanders or the USAF strongly at risk of mission or program failure, death, injury, legal jeopardy or unacceptable fraud, waste or abuse. T-1 waiver requests may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director, with the concurrence of the publication's approving official. (AFI 33-360)

**Tier 2 (T-2)**—Non-compliance has the potential to create moderate risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director. (AFI 33-360)

**Tier 3 (T-3)**—Non-compliance has a relatively remote potential to create risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the Wing/DRU/FOA/CC level. (AFI 33-360)

**United States Person**—A US citizen, an alien known by the DoD intelligence component concerned to be a permanent resident alien, an unincorporated association substantially composed of US citizens or permanent resident aliens, or a corporation incorporated in the United States unless it is directed and controlled by a foreign government or governments.

## Attachment 2

## PROPER USE MEMORANDUM (PUM) GUIDANCE FOR AIRBORNE AND DOD SATELLITE PLATFORMS

**A2.1.** PUM approval resides with MAJCOM/A2. PUM requests will be submitted to MAJCOM/A2 or AFISRA/CC via fax or email. MAJCOM/A2 and AFISRA/CC will coordinate PUM approval with MAJCOM/JA and/or AFISRA/JA. (T-1)

**A2.2.** PUM requests will include the following information: (1) Units involved (to include units involved in exploitation, (2) Timeframe, (3) Location, (4) Assets being used to conduct collection, and (5) Justification. (T-1)

**A2.3.** MAJCOM/A2 or AFISRA/CC will provide a timely response to requesting units that include any rules of engagement, if necessary. (T-1)