BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-104

16 APRIL 2007

Intelligence

OVERSIGHT OF INTELLIGENCE ACTIVITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This AFPD is available for downloading from the e-Publishing website at **www.e-publishing.af.mil/.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2RP
Supersedes AFI14-104, 14 April 2005

Certified by: AF/A2R (Mr. Kenneth K. Dumm)
Pages: 27

This instruction states the requirements for United States Air Force intelligence oversight activities. In this instruction, the use of the term intelligence refers to intelligence and counterintelligence units, activities, etc. It describes mandatory intelligence oversight-associated training requirements for Air Force components conducting intelligence activities. It also details how to identify, investigate, and report in the event of possible violations. This instruction implements Executive Order (EO) 12333 (part 2), *United States Intelligence Activities*; DOD Regulation 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*; DODD 5240.1, *DoD Intelligence Activities*; and Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*. This instruction does not apply to criminal investigative activities. For purposes of this instruction, the National Guard Bureau is a MAJCOM.

This instruction applies to all personnel assigned to Active Air Force, Air National Guard, and Air Force Reserve Command units engaged in intelligence activities as stated in paragraph **3.** Failure to observe the prohibitions and mandatory provisions specified in paragraphs **7.1.**, **9.6.2.**, **11.1.**, **11.2.2.**, **11.2.2.1.**, and **11.2.3.2.** of this Instruction (identified by **bold** font) by active duty Air Force members, AFRC members on active duty or inactive duty for training, and ANG members in federal status, is a violation of Article 92, Uniform Code of Military Justice. Violations by civilian employees of the same prohibitions and mandatory provisions may result in administrative disciplinary actions without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

See Attachment One for a glossary of references, abbreviations, acronyms, and terms. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF IMT 847, *Recommendation for Change of Publication*. Route AF IMT 847s from the field through the appropriate functional's chain of command. Field activities must send implementing publications to higher headquarters functional OPR for review and coordination before publishing.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. This revision updates the purpose statement to ensure inspectors general are cognizant of intelligence oversight (IO) policy and requirements (**1.**). It clarifies the training requirements of host nation employees (**3.1.**) and changes the title of the AFIWC to AFIOC (**3.3.**). It updates the responsibilities section by adding reporting requirements for SAF/GC and AF/A2 (**4.2.** and **4.3.**); deleting a separate AIA section for ACC; clarifying the responsibilities for commanders (**4.7.**); and adding separate sections for IO Monitors (**4.7.**), intelligence personnel (**4.8.**), inspectors (**4.9.**), and judge advocates/legal advisors (**4.10.**). It clarifies initial training requirements (**5.1.**); updates the SIPRNET and JWICS IO training website addresses (**5.2.** and **A2.4.**); and further explains pre-deployment training requirements (**5.3.**). It stipulates a timeframe for inspections of intelligence units (**6.3.**). It updates the quarterly reports section with new requirements based on the 2007 Defense Authorization Act by adding a section for AF/2 (**7.3.1.**), SAF/GC (**7.3.2.**), and SAF/IGX (**7.3.3.**) and expanding MAJCOM, FOA and DRU IO responsibilities (**7.3.4.**). It expands domestic imagery guidance (**9.**) and clarifies intelligence function in the force protection arena (**10.**). The change also delineates intelligence functions for each procedure identified in DOD 5240.1-R (**11.**); adds guidance for reporting incidentally acquired threat information (**12.**) and Internet usage (**13.**); and updates the reference section (**Attachment 1**).

1. Purpose. Intelligence oversight involves a balancing of two fundamental interests: obtaining the intelligence information required to protect national security and protecting individual rights guaranteed by the Constitution and the laws of the United States (US). The primary objective of the Intelligence Oversight Program is to ensure that units and staff organizations conducting intelligence activities do not infringe on or violate the rights of US persons. However, it is important to note that the program applies to all intelligence activities whether they deal with US person information or not. Commanders, inspectors general, and judge advocates at all levels need to be cognizant of intelligence oversight policies and requirements.

2. Conduct of Intelligence Activities. Information concerning capabilities, intentions, and activities of foreign governments and non-state actors is essential in decision-making for national defense and foreign relations. The measures used to acquire such information must be responsive to the legitimate needs of the US Government, and must be conducted in a manner that abides by the legal and constitutional rights of US persons.

2.1. This instruction directs all Air Force personnel potentially working with data collected on US persons to be knowledgeable of, and adhere to, the restrictions and procedures in DOD Regulation 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons* (DOD 5240.1-R) (see Index at Attachment Two, Training Program Primer).

2.2. This instruction neither authorizes any activity not previously authorized nor exempts anyone from any restrictions in DOD 5240.1-R.

3. Scope.

3.1. This instruction applies to all Air Force active duty, Air Force Reserve Command, and Air National Guard (when performing a federal function) intelligence units, staff organizations, and non-intelligence organizations that perform intelligence-related activities (e.g., Eagle Vision units) that could collect, analyze, process, retain, or disseminate information on US persons and those who exercise command over these units and organizations. It applies to all military and civilian personnel, to include Host Nation employees, assigned or attached to those units on a permanent or temporary basis, regardless of specialty or job function. Also, it applies to contractors or consultants if they are involved in activities subject to the procedures in DOD 5240.1-R. For Air Force Reserve Command, this AFI applies to Traditional Reservists, Air Reserve Technicians, Individual Mobilization Augmentees, and other Air Force Reserve Command members assigned or attached to intelligence units and staffs or performing intelligence-related activities. For the Air National Guard (ANG), it applies to all ANG members in a Title 10 or Title 32 status assigned or attached to intelligence units or staffs or performing intelligence-related activities.

3.2. This instruction also applies to non-intelligence units and staffs (e.g., Eagle Vision) when they are assigned an intelligence mission and to personnel doing intelligence work as an additional duty, even if those personnel are not assigned or attached to an intelligence unit or staff. The Senior Intelligence Officer of the major command (MAJCOM), field operating agency (FOA), or ANG determines applicability.

3.3. This instruction applies to Air Force units and staffs that conduct information operations activities and are components of intelligence organizations. For example, the Air Force Information Operations Center (AFIOC), which conducts information operations activities, is a component of the Air Intelligence Agency (AIA). As such, this instruction applies to the AFIOC. It also applies to all intel-

ligence personnel described in paragraph **3.1.**, above, who support information operations activities with products or services.

3.4. This instruction applies to non-intelligence units or staffs, such as Eagle Vision, running systems that acquire and disseminate commercial satellite products to intelligence units and staffs.

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

4. Responsibilities.

4.1. **Secretary of the Air Force, Inspector General (SAF/IG).** Chairs and is a voting member of the Air Force Intelligence Oversight Panel. Compiles inputs from SAF/GC, AF/A2 and MAJCOM/FOA/DRU Inspectors General to provide quarterly reports to the Assistant to the Secretary of Defense, Intelligence Oversight (ATSD(IO)) as specified in paragraph **7.**, below. Has access to all material necessary to perform assigned intelligence oversight responsibilities.

4.2. **Secretary of the Air Force, General Counsel (SAF/GC).** Legal counsel for all Air Force intelligence oversight issues. Provides advice to intelligence components on questions of legality or propriety, as required. Voting member of the Intelligence Oversight Panel. Provides input to SAF/IG in preparation of quarterly reports to the Assistant to the Secretary of Defense, Intelligence Oversight (ATSD(IO)) as specified in paragraph **7.** below. Has access to all material necessary to perform legal and intelligence oversight responsibilities.

4.3. **Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2).** Develops policy to ensure the proper supervision and control of Air Force intelligence activities. Coordinates with the ATSD(IO), the Air Force Inspector General, and the Air Force General Counsel on intelligence oversight matters. Voting member of the Intelligence Oversight Panel. Shall perform annual self-inspection, if necessary, per paragraph **6.4.** below. Provides input to SAF/IG in preparation of quarterly reports to the Assistant to the Secretary of Defense, Intelligence Oversight (ATSD(IO)) as specified in paragraph **7.** below. Ensures all units directly supporting Air Staff (AF/A2) comply with both the provisions of this instruction and those contained in all appropriate intelligence discipline-specific instructions.

4.4. **MAJCOMs, National Guard Bureau, and those FOAs and Direct Reporting Units (DRU) that perform Intelligence Activities as Defined in Paragraph 3.** Establish and maintain intelligence oversight programs to effect intelligence oversight and ensure all personnel assigned or attached to their intelligence components receive training according to paragraph **5.** Through their inspector general function, accomplish intelligence oversight inspections required by AFI 90-201, *Inspector General Activities*. Through their functional staffs, accomplish Staff Assistance Visits (SAV) as determined appropriate by the MAJCOM, DRU, or FOA commander. Note that intelligence oversight inspections of ANG intelligence units and staffs will normally be conducted by the gaining command. However, they may also be inspected by the National Guard Bureau Inspector General when gaining command inspection resources are not sufficient or available.

4.5. **AFOSI.** Ensure appropriate AFOSI units comply with both the provisions of this instruction and those contained in all appropriate counterintelligence discipline-specific instructions.

4.6. **Commanders/Directors of units that Perform Intelligence Activities as Defined in Paragraph 3.**

4.6.1. Be cognizant of IO procedures.

4.6.2. Ensure that IO rules and regulations are followed by intelligence personnel.

4.6.3. Levy tasks and missions in accordance with IO principles.

4.6.4. Designate in writing primary and alternate intelligence oversight monitors.

4.6.5. Ensure training programs as specified in paragraph **5.** and Attachment Two are conducted.

4.6.6. Ensure reporting directed in paragraph **7.** is completed.

4.7. **Intelligence Oversight Monitors.**

4.7.1. Implement an Intelligence Oversight training program, conduct intelligence oversight training as directed in paragraph **5.** and maintain records of this training.

4.7.2. Ensure copies of Executive Order 12333, *United States Intelligence Activities,* DODD 5240.1, *DOD Intelligence Activities*; DOD 5240.1-R; DODD 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight;* and this instruction are available to the unit in hard or electronic copy.

4.7.3. Submit quarterly reports as directed in paragraph **7.3.**

4.7.4. Perform a self-inspection in the final quarter of the calendar year if the unit has not been evaluated in the current calendar year by ATSD(IO), MAJCOM, FOA, or DRU inspectors general, or functional staffs accomplishing compliance-oriented SAVs, as directed by paragraph **6.**

4.7.5. Provide assistance in rendering collectability determinations on information acquired about US persons within 90 days, as detailed in paragraph **11.2.** If necessary, seek assistance from AF/A2.

4.8. **Intelligence Personnel.**

4.8.1. Know the mission of your organization.

4.8.2. Familiarize yourself with Procedures 1-4, 14 and 15 of 5240.1-R, this instruction, and any organization-specific instructions concerning IO.

4.8.3. Ensure you have taken your unit's IO training within 45 days of assignment/employment and annual refresher training as detailed in paragraph **5.**

4.9. **Inspectors General responsible for units that Perform Intelligence Activities as Defined in Paragraph 3.**

4.9.1. Know what intelligence units and/or non-intelligence units that perform intelligence activities come under your jurisdiction.

4.9.2. Understand your responsibilities as highlighted in Procedures 14 and 15 of DOD 5240.1-R.

4.9.3. Ensure you have the necessary clearances to perform your mission.

4.9.4. Understand the missions of each organization and which Procedures of DOD 5240.1-R relate to their missions.

4.9.5. Ensure organizations that perform intelligence functions have an established mechanism for reporting questionable activities.

4.9.6. Report questionable activities as detailed in paragraph **7.1.**

4.9.7. Submit quarterly reports as detailed in paragraph **7.3.**

4.9.8. Ensure you have taken the unit's IO training within 45 days of assignment/employment.

4.10. **Staff Judge Advocates/Legal Advisors responsible for units that Perform Intelligence Activities as Defined in Paragraph 3.**

4.10.1. Know what intelligence units and/or non-intelligence units that perform intelligence activities come under your jurisdiction.

4.10.2. Understand your responsibilities as highlighted in Procedures 14 and 15 of DOD 5240.1-R.

4.10.3. Ensure you have the necessary clearances to provide legal advice.

4.10.4. Understand the missions of each organization and which Procedures of DOD 5240.1-R relate to their missions.

4.10.5. Ensure you have taken the unit's IO training within 45 days of assignment/employment.

4.10.6. Report questionable activities as detailed in paragraph **7.1.**

5. Training.

5.1. **Initial Training.** Technical training centers will provide initial intelligence oversight training to all Air Force intelligence personnel as part of their technical training. Intelligence oversight monitors will provide intelligence oversight training to all personnel identified in paragraph **3.** within 45 days of arrival to their newly assigned units, to include permanent change of station. Intelligence Oversight Monitors will also provide orientation training to all staff judge advocates and inspectors general within 45 days of employment or assignment. Training will cover, at a minimum, the matters set out in Attachment Two.

5.2. **Annual Refresher Training.** Intelligence oversight monitors will provide annual refresher training to all Air Force personnel and other personnel identified in paragraph **3.**, who are assigned or attached to, or employed by, Air Force intelligence components. This training will cover, at a minimum, the matters set out in Attachment Two. Units will keep records of personnel training. The ATSD(IO) web sites (NIPRNET: **www.dod.mil/atsdio**; SIPRNET: **www.atsdio.ismc.sgov.gov/atsdio/**; or JWICS: **www.atsdio.ismc.ic.gov/atsdio**/) are highly recommended as a source of training materials, to include a computer-based training program (on the SIPRNET and JWICS sites and available on CD), as well as the basic references governing intelligence oversight listed in para **A3.1.4.** (See Attachment Two for a primer on intelligence oversight training.) Sample training materials are also available at the Intelligence Oversight Community of Practice (CoP) on the Air Force Portal (NIPRNET: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-IN-AF-15**)).

5.3. **Pre-Deployment Training.** Intelligence oversight monitors will ensure personnel deploying to another duty location will retain currency for the duration of the deployment or temporary duty (TDY). If currency will lapse during the deployment or TDY, refresher training will be provided and fulfill the annual training requirement.

6. Compliance Inspection Guidance. Inspectors, SAV team members, and units will follow the guidance in Attachment Three of this AFI. They will assess the intelligence unit's and staff's compliance with

the rules and procedures pertaining to collecting, retaining, and disseminating intelligence on US persons and the adequacy of intelligence oversight programs.

6.1. MAJCOM, FOA, and DRU inspectors general shall use Attachment Three when accomplishing the compliance inspection item inspections required by AFI 90-201, Attachment Six.

6.2. Functional representatives shall use Attachment Three when accomplishing compliance-oriented SAVs.

6.3. Intelligence units will be evaluated by either ATSD(IO) or MAJCOM, FOA, or DRU inspectors general during each Unit Compliance or Operational Readiness Inspection to achieve a nominal periodicity of three years. It is not the intent of this requirement to drive a separate IO inspection. Report results IAW paragraph **7.3.3.**

6.4. Intelligence unit commanders or chiefs of intelligence staffs who have not been evaluated in the current calendar year by ATSD(IO), MAJCOM, FOA, or DRU inspectors general, or functional staffs accomplishing compliance-oriented SAVs, shall perform a self-inspection, using the checklist in Attachment Three, in the final quarter of each calendar year. The results shall be forwarded to MAJCOM, FOA, or DRU inspector general. The MAJCOM, FOA, and DRU inspectors general shall consolidate the results and provide a report to SAF/IGI no later than 5 Jan of the next calendar year. Results of ANG inspections will also be provided to the National Guard Bureau Inspector General.

7. Inquiries and Reporting.

7.1. **Reporting Questionable Activities. Air Force agencies, units, and personnel must report any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, *United States Intelligence Activities*, or applicable DOD policy, including DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* this instruction, and/or other Air Force policy documents and instructions.** Such a violation is not a "questionable activity" in this context unless there is some nexus between the activity and an intelligence function. SAF/GCM can provide assistance in making such determinations.

7.1.1. Air Force agencies, units, and personnel must report questionable activities to the SAF/GC, SAF/IG, the DOD General Counsel or ATSD(IO). Use of the supervisory chain or chain of command is encouraged to facilitate such reports where feasible. 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. This report must be made regardless of whether a criminal or other investigation has been initiated.

7.1.2. MAJCOMs/FOAs/DRUs similarly will report questionable activities to SAF/IG through their inspectors general, providing information copies of the report to SAF/GC and AF/A2.

7.1.3. SAF/IG and SAF/GC will report immediately to DOD General Counsel and the ATSD(IO) questionable activities of a serious nature. Any such reports, and the quarterly reports described in paragraph **7.3.** below, are exempt from Report Control Symbol (RCS) licensing procedures according to AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections.*

7.2. **Inquiries.** Air Force agencies and units will inquire into any questionable activity reported under paragraph **7.1.**, to the extent necessary to determine whether the reported activity violates law, executive order, Presidential directive, DOD directive or policy, or Air Force instruction or policy. Conduct all inquiries as quickly as possible and forward the results through command channels to SAF/IG. Officials responsible for inquiries may obtain additional assistance from within the component concerned or from other DOD components, when necessary, to complete inquiries in a timely manner. SAF/IG and SAF/GC must have all information necessary to evaluate questionable activity for compliance with law or policy, regardless of classification or compartmentation.

7.3. **Submitting Quarterly Reports.**

7.3.1. **AF/A2** must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI five calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a quarterly report to ATSD(IO), which will be signed by SAF/IG, SAF/GC, and AF/A2. Inputs must include:

7.3.1.1. A summary of any substantive Air Force-level change(s) to intelligence oversight programs, including changes to supporting training programs, and the reason for the change(s). Attach a copy of the directive or policy directing the change.

7.3.1.2. A summary of any Air Force-level changes to published directives or policies concerning intelligence, or intelligence-related activities and the reason for the changes. Attach a copy of the directive or policy.

7.3.2. **SAF/GC** must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI five calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a quarterly report to ATSD(IO), which will be signed by SAF/IG, SAF/GC, and AF/A2. Inputs must include:

7.3.2.1. A description of any intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the quarter, as well as any actions taken as a result of the violations.

7.3.2.2. The status of any ongoing Procedure 15 inquiries and additional matters pertinent to the Air Force intelligence oversight programs.

7.3.3. **SAF/IGX** must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI five calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a quarterly report to ATSD(IO), which will be signed by SAF/IG, SAF/GC, and AF/A2. Inputs must include:

7.3.3.1. A summary of any Air Force-level changes to published directives or policies concerning counterintelligence or counterintelligence-related activities and the reason for the changes. Attach a copy of the directive or policy.

7.3.4. Each MAJCOM, FOA, or DRU Inspector General responsible for an Air Force organization or staff subject to this instruction must submit quarterly inputs to SAF/IGI. Inputs are due at SAF/IGI five calendar days after the end of each quarter. SAF/IGI will consolidate all inputs into a quarterly report to ATSD(IO), which will be signed by SAF/IG, SAF/GC, and AF/A2. Inputs must include:

7.3.4.1. A description of any questionable activities (not confined to reporting on US persons-associated violations) identified during the quarter and reference to any report previously made concerning them (see paragraph **7.1.**).

7.3.4.2. Actions taken regarding such activities.

7.3.4.3. A list of intelligence oversight evaluations or inspections by unit and location and a paragraph summarizing the results or trends from these evaluations or inspections. Include any questionable activity discovered, the familiarity of personnel with intelligence oversight requirements, and the adequacy of organization intelligence oversight programs, structure, and processes. Include results of inspections conducted by any outside agency such as ATSD(IO) (include unit and location), and planned next-quarter intelligence oversight inspections (provide unit and location). If any evaluations or inspections reveal deficiencies, note the corrective action(s) taken.

7.3.4.4. On the report for the last quarter of each calendar year, the status of self-inspections conducted IAW paragraph **6.** above.

7.3.4.5. The MAJCOM, FOA, or DRU report for the last quarter of each calendar year shall include a list of the units and staffs for which the MAJCOM, FOA, or DRU has intelligence oversight and inspection requirements (specifying MAJCOM, parent organization, unit designation, and location). **Note:** This list may be classified due to unit's mission. Ensure report is marked and handled accordingly.

7.3.4.6. Significant oversight activities undertaken during the quarter and any suggestions to improve the intelligence oversight program are also encouraged.

8. Air Force Intelligence Oversight Panel. The Panel consists of SAF/IG (chair), SAF/GC, and AF/A2. Its functions are to review the legality and propriety of Air Force intelligence activities, review the adequacy of guidance for Air Force intelligence unit and staff intelligence oversight programs, and review the state of intelligence oversight activities, taking or recommending necessary actions, as appropriate.

9. Domestic Imagery. Air Force 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, commercial or tactical) 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.

9.1. Collecting information on specific targets inside the US raises policy and legal concerns that require careful consideration, analysis and coordination with legal counsel. Therefore, Air Force components should use domestic imagery only when there is a justifiable need to do so, and then only in accordance with EO 12333, the National Security Act of 1947, as amended, DOD Regulation 5240.1-R, and this instruction. The following generally constitute legally valid requirements for domestic imagery:

9.1.1. Natural Disasters. Requirements to target 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.

9.1.2. 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.

9.1.3. 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.

9.1.4. Exercise, Training, Testing, or Navigational Purposes. Requirements for imagery coverage in support of system or satellite calibration, algorithm or analytical developments and training or weapon systems development or training.

9.2. **Domestic Imagery from National Satellites.** The National Geospatial-Intelligence Agency (NGA) is responsible for the legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites. Air Force components must follow policy and procedures established in Geospatial Intelligence Policy Series, Chapter 1 – Imagery Policy, Section 8, Part B. *Domestic Imagery.* Air Force components must submit a Proper Use Memorandum (PUM) each year to NGA that defines the requirements for domestic imagery, outlines its intended use, and includes 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. For ad hoc domestic imagery requests (i.e., those that fall outside the scope of an approved PUM), Air Force components must submit a Domestic Imagery Request (DIR) to NGA.

9.3. **Domestic Imagery from Airborne Platforms.** An approved PUM must be on file with the appropriate Combatant Command or Military Service (or delegated/designated sub-component PUM authority) before airborne platforms can be tasked to collect domestic imagery. These PUMs must be in accordance with applicable Defense Intelligence Agency (DIA) policy and guidance, applicable executive orders, and DOD regulations. 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 platforms must be coordinated with USNORTHCOM to ensure compliance with proper use provisions. For ad hoc domestic imagery requests (i.e., those that fall outside the scope of an approved PUM), Air Force components must submit a PUM request through their MAJCOM to the designated approval authority. (See paragraph **9.6.** for an exception to this paragraph.)

9.4. **Domestic Imagery from Commercial Satellites.** Air Force intelligence components can obtain domestic commercial imagery without higher-level approval for valid mission purposes such as training or testing on federally owned and operated ranges, calibration-associated systems development activities, and domestic disaster relief operations. However, an internal memorandum for record (MFR) describing the purpose of the domestic imagery and the component official approving the use should be retained on file. If obtained imagery specifically identifies a US person (e.g., private property), then the rules and procedures contained in DOD 5240-1.R, in particular those regarding retention, must be followed. Air Force intelligence components must not give the appearance of collecting, exploiting or disseminating commercial imagery or imagery associated products for other than approved mission purposes.

9.5. **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. (See paragraph **11.4.**) Unless otherwise approved, domestic imagery must be withheld from all general access database systems (e.g., Intelink).

9.6. **Fighter, Bomber and Unmanned Aircraft System (UAS) Navigational/Target Training activities.**

9.6.1. Air Force 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. For example, imagery could be collected of a private structure so that the imagery can be used as a visual navigational aid or to simulate targeting during training. However, imagery may not be collected for the purpose of gathering any specific information about a US person or private entity, without consent, nor may stored imagery be retrievable by reference to US person identifiers.

9.6.2. **Air Force UAS operations, exercise and training missions will not conduct 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 (CBP), Federal Bureau of Investigations (FBI), US Immigration and Customs Enforcement (ICE), and the US Coast Guard, will handle any such data collected.

10. Force Protection.

10.1. As a general rule, force protection operations within the United States are a law enforcement responsibility, including Air Force Security Forces and the AFOSI in their criminal law enforcement capacity. Air Force Intelligence components must focus on analyzing all-source information concerning threats to DOD missions, people, or resources arising from transnational terrorists and opposing military forces in support of force protection decisions and operations. If during the course of routine intelligence activities and authorized missions, Air Force 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 paragraph **12.** of this instruction.

10.2. Air Force intelligence components that have been assigned a force protection mission may only collect information on US persons in accordance with the procedures in this instruction and in DOD 5240.1-R. Coordinate with the AFOSI prior to collecting information on any US individual/domestic group for force protection purposes.

10.3. Air Force intelligence assets assigned a mission to support force protection that are part of the entity that has responsibility for countering the threat may assist in fusing law enforcement, counterintelligence, and intelligence information in support of force protection (e.g., antiterrorism and/or law enforcement activities), consistent with intelligence oversight procedures.

11. Procedural Guidance. Air Force 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 and this instruction.

11.1. **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 and this instruction.**

11.2. **Collection.** Information about US persons may be collected if it falls within one or more of the thirteen categories of information specified in Procedure 2, DOD 5240.1 -R. That procedure also sets forth general criteria governing the means used to collect such information.

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

11.2.2. Information 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 the receiving unit is uncertain as to whether the US person information may be collected and permanently retained, it should seek advice through the chain of command. The unit/MAJCOM Intelligence Oversight Monitor must provide assistance in rendering collectability determinations. When appropriate, assistance may be requested from AF/A2. **In no event may a determination whether information is collectible take longer than a total of 90 days.**

11.2.2.1. **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.**

11.2.2.2. Even though information may not be collectible, it may be retained so long as it is necessary to transfer it to another DOD entity or government agency to whose function it pertains, but no longer.

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

11.2.3.1. **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.

11.2.3.2. **Collection Within the United States. Within the United States, 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 Department of Defense, or a component thereof. Collection by other than overt means may only be accomplished if all of the following criteria are satisfied:

11.2.3.2.1. The foreign intelligence sought must be significant and not being collected for the purpose of acquiring information concerning the domestic activities of any US person;

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

11.2.3.2.3. The collection of such foreign intelligence has been coordinated with the FBI; and,

11.2.3.2.4. The use of other than overt means has been approved by the Secretary of the Air Force. Authority to approve such requests is hereby delegated to the AF/A2. AF/A2 will provide a copy of any such approval to the Undersecretary of Defense for Intelligence (USD(I)).

11.3. **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 information that is required by law to be retained. "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.

11.3.1. 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 Air Force intelligence component concerned.

11.4. **Dissemination.** US person information in the possession of an Air Force intelligence component may be disseminated pursuant to law, a court order, or in accordance with the following criteria:

11.4.1. The information was properly collected or retained.

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

11.4.2.1. 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.

11.4.2.2. 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.

11.4.2.3. 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.

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

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

11.5. **Electronic Surveillance.**

11.5.1. Electronic surveillance for counterintelligence purposes must be conducted in accordance with instructions and procedures promulgated by the Commander, AFOSI, approved by the Secretary of the Air Force, and contained in Signals Intelligence (SIGINT) directives, including United States Signals Intelligence Directive (USSID) 18.

11.5.2. Requests to conduct electronic surveillance 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 appropriate approval. AF/A2 will coordinate with SAF/GCM.

11.6. **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/GCM (foreign intelligence).

11.6.1. 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.

11.6.2. Within the US, an Air Force 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.

11.6.3. Outside the US, concealed monitoring may be conducted on installations and facilities owned or leased by the DOD. Monitoring outside such facilities shall 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).

11.7. **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. Nor does any intrusion authorized as necessary to accomplish lawful electronic surveillance constitute a physical search.

11.7.1. **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. Air Force intelligence components may not otherwise conduct nonconsensual physical searches within the US for foreign intelligence or counterintelligence purposes.

11.7.2. **Physical Searches Outside the United States.**

11.7.2.1. 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.

11.7.2.2. Physical searches of the person or property of US persons, other than active duty military personnel, may be conducted only with the approval of the Attorney General.

11.7.2.3. 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.

11.8. **Searches and Examination of Mail.**

11.8.1. Applicable postal regulations do not permit the Air Force to detain or open first class mail within US postal channels for foreign intelligence or for counterintelligence purposes. 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.

11.8.2. Air Force 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 in accordance with 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.

11.8.3. Air Force 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.

11.8.4. 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.

11.8.5. **Mail Covers.** The Commander, AFOSI may request US postal authorities examine mail in US postal channels for counterintelligence purposes. 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, in accordance with appropriate law and procedures of the host government and any SOFA that may be in effect.

11.9. **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.

11.9.1. Physical surveillance for counterintelligence purposes, both within and outside the US, shall be approved and conducted in accordance with DOD 5240.1-R and procedures established by the Commander, AFOSI.

11.9.2. Physical surveillance for foreign intelligence purposes shall be approved and conducted in accordance with DOD 5240.1-R and procedures established by the AF/A2, or his designee.

11.10. **Undisclosed Participation in Organizations.** Participation by an employee of an Air Force 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 in accordance with the requirements in subparagraphs **11.10.1.** and **11.10.2.** Undisclosed participation that occurs outside a DOD installation must be coordinated with the FBI (within the US), CIA (outside the US), or other agency as required. Intelligence component employees do not require permission to participate in organizations for solely personal purposes.

11.10.1. **Undisclosed** participation for counterintelligence purposes must be approved by Commander, AFOSI, and conducted according to DOD 5240.1-R and procedures established by the Commander, AFOSI, or his designee.

11.10.2. Undisclosed participation for foreign intelligence purposes must be approved by AF/A2 and conducted according to DOD 5240.1-R and procedures established by AF/A2.

11.11. **Contracting for Goods and Services.** Procedure 11, DOD 5240.1-R applies to contracting or other arrangements with US persons for the procurement of goods and services by or for an Air Force intelligence component within the US. 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 of section **11.10.** apply.

11.11.1. **Contracts with academic institutions.** Air Force intelligence components may not enter into contracts for goods or services with academic institutions before the fact of sponsorship

by an Air Force intelligence component is disclosed to appropriate officials of the academic institution.

11.11.2. **Contracts with commercial organizations, private institutions and individuals.** Air Force intelligence components may contract with such entities within the US without revealing the sponsorship of the intelligence component only if:

11.11.2.1. 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

11.11.2.2. There is a written determination by the Secretary or Under Secretary of the Air Force that the sponsorship by an Air Force intelligence component must be concealed to protect the activities of the intelligence component concerned.

11.12. **Assistance to Law Enforcement.**

11.12.1. **Cooperation with law enforcement authorities.** Subject to the limitations of paragraph **11.12.2.** of this Instruction, Air Force intelligence components may cooperate with law enforcement authorities IAW DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, for the purpose of:

11.12.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities and/or

11.12.1.2. Protecting DOD employees, information, property and facilities.

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

11.12.2. **Types of permissible assistance.** Air Force intelligence components may only provide the types of assistance to law enforcement authorities delineated below. Assistance may not be provided for participation in activities that would not be permitted under this instruction.

11.12.2.1. **Violations of US federal law.** Incidentally acquired information reasonably believed to indicate a violation of federal law shall be provided to appropriate federal law enforcement officials through AFOSI channels.

11.12.2.2. **Other violations of law.** Information incidentally acquired during the course of Air Force counterintelligence activities reasonably believed to indicate a violation of state, local, or foreign law will be provided to appropriate officials in accordance with procedures established by the Commander, AFOSI. Information incidentally acquired during the course of Air Force 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 in accordance with procedures established by the AF/A2, or his designee, for investigation or referral to the appropriate law enforcement agency. Information covered by this paragraph includes US person information. (See also paragraph **12.**)

11.12.2.3. **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 SAF/IG and the concurrence of SAF/GC.

11.12.2.4. **Assistance of Air Force intelligence personnel.** Air Force intelligence personnel may be assigned to assist federal law enforcement authorities with the approval of AF/A2 and the concurrence of SAF/GC. Under certain exigent circumstances (i.e., when lives are in danger), Air Force intelligence personnel may be assigned to assist state and local law enforcement authorities, provided such assistance has been approved by the Deputy Chief of Staff, Manpower and Personnel (AF/A1) and SAF/GC.

11.13. **Experimentation on Human Subjects for Intelligence Purposes.** Air Force 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 in accordance with procedures established by AF/SG to safeguard the welfare of subjects.

11.13.1. 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.

11.13.2. Experimentation is conducted on behalf of an Air Force intelligence component if it is conducted under contract to Air Force or to another DOD component for the benefit of the Air Force or at the request of the Air Force regardless of the existence of a contractual relationship.

11.13.3. 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.

12. Reporting of Incidentally Acquired Threat Information. If during the course of routine activities and authorized missions, Air Force intelligence components 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) that information must be passed to appropriate authorities.

12.1. In the event that the threat information involves an imminent threat to life or serious property damage, the Air Force intelligence component will immediately notify appropriate entities with responsibility for countering the threat (e.g., Base Command Section, Security Forces, FBI, Municipal Police Department, etc.). The Air Force intelligence component must also immediately notify AFOSI. In the event immediate notification of the local AFOSI unit is not possible, the Air Force intelligence component will notify the AFOSI Global Watch Center, DSN: 857-0393, Commercial 240-857-0393, or Commercial Toll Free 1-877-246-1453.

12.2. Absent imminent threat, reporting should be limited to AFOSI who will determine whether further reporting will unacceptably compromise potential investigative or operational activities and forward to other authorities as appropriate.

12.3. 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.

13. The Internet. While much of the information posted on the Internet is publicly available, Air Force intelligence components must have an official mission requiring it before collecting, retaining, or dissem-

inating even 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 SIPRNET and JWICS.

DAVID A. DEPTULA, Lt Gen, USAF
DCS, Intelligence, Surveillance and Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

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

Defense Authorization Act for Fiscal Year 2007 (10 United States Code 427), Section 932, *Annual Reports on Intelligence Oversight Activities of the Department of Defense*

Department of Defense Directive 2000.12, *DOD Antiterrorism (AT) Program*, 18 August 2003

Department of Defense Directive 5148.11, *Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))*, 21 May 2004

Department of Defense Directive 5240.1, *DOD Intelligence Activities*, 25 April 1988

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

Department of Defense Regulation 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* December 1982

Department of Defense Directive 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, 15 January 1986

Air Force Policy Directive (AFPD) 10-8, *Homeland Defense and Civil Support*, 7 September 2006

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

Air Force Policy Directive (AFPD) 31-2, *Law Enforcement*, 6 May 1994

Air Force Instruction (AFI) 10-245, *Air Force Antiterrorism (AT) Standards*, 21 June 2002

Air Force Instruction (AFI) 10-801, *Assistance to Civilian Law Enforcement Agencies*, 15 April 1994

Air Force Instruction (AFI) 14-119, *Intelligence Support to Force Protection,* 6 January 2004

Air Force Instruction (AFI) 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

Air Force Manual (AFMAN) 37-123, *Management of Records,* 31 August 1994

Air Force Instruction (AFI) 71-101, Volume 1, *Criminal Investigations,* 1 December 1999

Air Force Instruction (AFI) 71-101, Volume 4, *Counterintelligence*, 1 August 2000

Air Force Instruction (AFI) 90-201, *Inspector General Activities*, Incorporating Through Change 2, 29 November 2006

National Geospatial-Intelligence Agency Imagery Policy Series, Section 5, *National Airborne Imagery Policy,* December 2004, and Section 8. Part B, *Domestic Imagery*, January 2006

United States Signals Intelligence Directive (USSID) 18, 27 July 2003

Title 50, Chapter 36, United States Code, *Foreign Intelligence Surveillance Act of 1978*

Deputy Secretary of Defense Memorandum, *Collection, Reporting, and Analysis of Terrorist Threats to DOD Within The United States*, 2 May 2003

Deputy Secretary of Defense Memorandum, *Threats to the Department of Defense*, 30 March 2006

Deputy Secretary of Defense Memorandum, *DOD Integrated Threat Reporting Working Group,* 12 October 2006

Deputy Secretary of Defense Memorandum, *Interim Guidance for the Domestic Use of Unmanned Aircraft Systems,* 28 September 2006

USD(CI&S) Memo, *Authority to Collect Information on Domestic Terrorist and Other Groups Committing Illegal Acts that Pose a Threat to the Department of Defense,* 25 May 2005

Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, 5 April 1979 with *Supplement to the 1979 FBI/DOD Memorandum of Understanding: Coordination of Counterintelligence Matters Between FBI & DOD*, 20 June 1996

Abbreviations and Acronyms

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

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

AFIOC—Air Force Information Operations Center

AFOSI—Air Force Office of Special Investigations

AIA—Air Intelligence Agency

AFI—Air Force Instruction

ANG—Air National Guard

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

CBP—United States Customs and Border Patrol

CIA—Central Intelligence Agency

CoP—Community of Practice

DIA—Defense Intelligence Agency

DIR—Domestic Imagery Request

DOD—Department of Defense

DRU—direct reporting unit

EO—executive order

FBI—Federal Bureau of Investigation

FOA—field operating agency

ICE—United States Immigration and Customs Enforcement

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

NGA—National Geospatial-Intelligence Agency

NIPRNET—Unclassified but Sensitive (N-level) Internet Protocol Router Network

PUM—Proper Use Memorandum

UAS—Unmanned Aircraft System

USD(I)—Undersecretary of Defense for Intelligence

USNORTHCOM—United States Northern Command

SAF/GC—Secretary of the Air Force General Counsel

SAF/IG—Secretary of the Air Force Inspector General

SAV—Staff Assistance Visit

SIGINT—Signals Intelligence

SIPRNET—Secret Internet Protocol Router Network

SOFA—Status of Forces Agreement

TDY—temporary duty

USSID—United States Signals Intelligence Directive

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.

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

Domestic Imagery Request (DIR)—A 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. It generally reflects ad hoc requirements for domestic imagery.

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.

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.

Proper Use Memorandum—A memorandum signed annually by an organization's Certifying Government Official that defines the organization's domestic imagery requirements and intended use. It also contains a proper use statement acknowledging awareness of the legal and policy restrictions regarding domestic imagery.

Questionable Activity—Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, *United States Intelligence Activities*, or applicable DOD policy, including DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons,* this AFI, and/or other Air Force policy documents and instructions. Such a violation is not a "questionable activity" in this context unless there is some nexus between the activity and an intelligence function.

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

TRAINING PROGRAM PRIMER

A2.1. Introduction. The material below is provided as a core curriculum for an intelligence unit or staff intelligence oversight program. It is intended to provide a common sense perspective on this important but often seemingly complex subject.

A2.2. Background. Intelligence Oversight has become a commonly understood term referring to a group of laws, directives, and associated institutional bodies designed to ensure that US intelligence activities are conducted legally and properly, and do not infringe on the rights of US persons. For the Air Force, there are two primary governing directives: DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect US Persons,* and AFI 14-104, *Oversight of Intelligence Activities*.

A2.3. Tenets. Air Force intelligence personnel should understand the following central tenets of the Air Force intelligence oversight program:

A2.3.1. **Scope.** The Air Force intelligence oversight program pertains to all personnel assigned or attached to intelligence units or staffs that could collect, analyze, process, retain, or disseminate information on US persons. These include active, reserve, guard, civilian, TDY and contractor personnel. See Terms in Attachment One for definition of US person. Further, the program pertains to any person when tasked to perform an intelligence mission regardless of their unit of assignment.

A2.3.2. **Permissible Activities.** Air Force intelligence units and staffs can collect, retain, and disseminate intelligence on US persons only if it is necessary to the conduct of a function or mission assigned the collecting component and only if it falls within one of the thirteen categories listed under DOD 5240.1-R, Procedure 2. In the US, it is not generally within the mission of military intelligence units to collect information on US persons (this would normally be within the mission of counterintelligence units). As such, although some information on US persons may be "publicly available" (one of the 13 categories referred to above), this does not obviate the unit mission/function requirements.

A2.3.3. **Collection Techniques.** There are very specific procedures and restrictions governing collecting intelligence on US persons by methods such as electronic surveillance or physical search or participation in activities of private organizations. (DOD 5240.1-R, Procedures 5-11)

A2.3.4. **Law Enforcement Assistance.** There are very specific procedures and restrictions on providing intelligence support to law enforcement agencies. (DOD 5240.1-R, Procedure 12)

A2.3.5. **Questionable Activities.** Intelligence oversight is much broader than just collecting, retaining and disseminating intelligence on US persons. Unit members or staff personnel are required to report "questionable activities," defined "as any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, *United States Intelligence Activities*, or applicable DOD policy, including DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons."*

A2.3.6. **Reporting**. Personnel assigned to intelligence units or staffs must report any possible intelligence oversight-associated violations or irregularities to the Judge Advocate General (JAG) or Intelligence Oversight Monitor, the wing or base inspector general, the Air Force General Counsel, the Air

Force Inspector General, the DOD General Counsel or ATSD(IO). Use of the supervisory chain or chain of command is encouraged to facilitate such reports where feasible. 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, senior intelligence officers at the same level. (DOD 5240.1-R, Procedure 15 and this instruction, paragraph **7.2.**)

A2.3.7. **The Internet.** While much of the information posted on the Internet is publicly available, an intelligence professional acting in an official capacity still must have the official mission before collecting, retaining, or disseminating even 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 SIPRNET and JWICS. (DOD 5240.1-R, Procedure 10 and 11)

A2.4. Reminder. Even though most intelligence personnel are not "collectors," most do retain and disseminate intelligence. Some personnel, such as those working with domestic imagery collection or information warfare programs, may need a more in-depth understanding of select aspects of intelligence oversight rules and procedures. All are encouraged to periodically check the Air Force Intelligence Oversight Community of Practice (CoP) on the Air Force Portal (NIPRNET: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-IN-AF-15**) as well as the web site maintained by the Assistant to the SECDEF, Intelligence Oversight (NIPRNET: **www.dod.mil/atsdio**; SIPRNET: **www.atsdio.ismc.sgov.gov/atsdio/**; or JWICS: **www.atsdio.ismc.ic.gov/atsdio/**) for soft copies of the basic intelligence oversight references, additional training aids/software, a list of frequently asked questions/intelligence oversight examples, and other useful information. Other techniques that can be used to raise awareness are poster campaigns/visual aids and messages posted in newsletters or on bulletin boards.

A2.5. Index - DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence That Affect United States Persons*

A2.5.1. **Procedure 1- General Provisions**

A2.5.2. **Procedure 2 - Collection of Information about US Persons.** Note - information that identifies a US person may be collected only if it is necessary to the conduct of a function assigned to the collection component, and only if it falls within one of the categories listed in DOD 5240.1-R, Procedure 2.

A2.5.3. **Procedure 3 - Retention of Information about US Persons**

A2.5.4. **Procedure 4 - Dissemination of Information about US Persons**

A2.5.5. **Procedure 5 - Electronic Surveillance.** Note-this procedure also applies to signals intelligence activities. See the classified annex to EO 12333 and USSID 18 for more information.

A2.5.6. **Procedure 6 - Concealed Monitoring**

A2.5.7. **Procedure 7 - Physical Searches**

A2.5.8. **Procedure 8 - Searches and Examination of Mail**

A2.5.9. **Procedure 9 - Physical Surveillance**

A2.5.10. **Procedure 10 - Undisclosed Participation in Organizations**

A2.5.11. **Procedure 11 - Contracting for Goods and Services Without Revealing the Sponsorship by the Intelligence Component**

A2.5.12. **Procedure 12 - Provision of Assistance to Law Enforcement Authorities**

A2.5.13. **Procedure 13 - Experimentation on Human Subjects for Intelligence Purposes**

Note - Procedures 5 - 13 contain detailed rules, prohibitions, and approval processes for specialized collection methods and techniques. The majority of Air Force intelligence units and staffs will never be required or authorized to conduct the activities described in these procedures, all of which require approval by specific higher level officials. Judge Advocate General or General Counsel authorities should be consulted on any matter pertaining to procedures 5 - 13.

A2.5.14. **Procedure 14 - Employee Conduct**

A2.5.15. **Procedure 15 - Identifying, Investigating, and Reporting Questionable Activities**

Note 1 - see discussion of "reporting " above, and in "questionable activities" and "reporting" provisions in this instruction, paragraphs **7.1.** and **7.2.**

Note 2 - Air Force intelligence units and staffs should consider using the ATSD(IO)-produced, web-based intelligence oversight training program as part of their unit or staff intelligence oversight program.

Note 3 – **Attachment 3** to this instruction includes detailed information about individual knowledge of intelligence oversight necessary to pass an intelligence oversight inspection. Use of it as an additional training aid is recommended.

Attachment 3

INSPECTION GUIDANCE

Inspectors, staff assistance visit (SAV) team members, and units should follow this checklist when assessing the adequacy of intelligence oversight programs. Failure of a critical item requires an "Unsatisfactory" rating for the unit intelligence oversight program. Results and corrective actions will be reported in accordance with paragraph **7.3.4.**

A3.1. Administrative.

A3.1.1. Ensure the primary and alternate intelligence oversight monitors are appointed in writing.

(Note: This is a non-critical item. If a unit is not compliant, provide a 10-day answerable action item to the unit to update their paperwork.)

A3.1.2. Ensure initial and annual training is accomplished and those records of training accomplished are available and current.

(Note: This is a **critical item**. Failure occurs if more than 25% of the unit personnel are not current on their training.)

A3.1.3. Ensure initial and annual training lesson plans cover the minimum objectives outlined in Attachment Two.

(Note: This is a non-critical item. If a unit is not compliant, the training lesson plan must be updated within 30 days of the inspection.)

A3.1.4. Ensure copies of DOD 5240.1-R, DODD 5148.11, and this instruction are available to the unit in hard or electronic copy.

(Note: This is a non-critical item. If a unit is not compliant, provide a 10-day action item to the unit to correct the deficiency.)

A3.1.5. Ensure units who have not been evaluated in the current calendar year by ATSD(IO), MAJCOM, FOA, or DRU inspectors general, or functional staffs accomplishing compliance-oriented SAVs, perform a self-inspection, using the checklist in Attachment Three in the final quarter of each calendar year. Ensure results are forwarded to MAJCOM, FOA, or DRU inspector general.

(Note: This is a non-critical item. If a unit is not compliant, provide a 10-day action item to the unit to correct the deficiency.)

A3.2. Functional.

A3.2.1. Determine if unit members and staff personnel are aware of the applicability of intelligence oversight limitations to them.

(Note: This item is a **critical item**. A minimum of 75 % of individuals must be aware of the meaning and limitations for this item to be satisfactory.)

A3.2.2. Determine if unit members and staff personnel are aware of the circumstances under which intelligence can be collected, retained, and disseminated on US persons (e.g., information obtained with consent).

(Note: This is a **critical item**. A minimum of 75% of individuals must be aware that DOD 5240.1-R describes the circumstances under which information on US persons may be collected for this item to be satisfactory. See Attachment Two and DOD 5240.1-R, Procedure 2 for more details.)

A3.2.3. Determine if unit members and staff personnel are aware that there are specific procedures and restrictions governing the collection of intelligence on US persons by methods such as electronic surveillance or physical surveillance

(Note: This is a **critical item**. A minimum of 75 % of individuals must be aware of the existence of such limitations and sources of information concerning them for this item to be satisfactory. See Attachment Two, and DOD 5240.1-R, Procedures 5-11 for more details.)

A3.2.4. Determine if unit members and staff personnel are aware that there are specific procedures and restrictions on providing intelligence support to law enforcement agencies.

(Note: This is a **critical item**. A minimum of 75 % of individuals must be aware of the existence of such limitations for this item to be satisfactory. See Attachment Two, and DOD 5240.1-R, Procedure 12 for more details.)

A3.2.5. Determine if unit members and staff personnel are aware that they are required to report "questionable activities" conducted by intelligence components that constitute possible violations of law, directive, or policy. Also determine if personnel are aware that using the chain of command for reporting "questionable activities" is encouraged where feasible.

(Note: This is a **critical item**. A minimum of 75 % of individuals must be aware of the requirement to report "questionable activities" and also be aware that using the chain of command is the preferable reporting mechanism for this item to be satisfactory. See Attachment Two, and DOD 5240.1-R, paragraph A.2.3.6. and Procedure 15 for more details.)

A3.2.6. Determine if unit members and staff personnel understand that "US Person" pertains to associations, corporations, and resident aliens as well as US citizens.

(Note: This is a **critical item**. A minimum of 75 % of individuals must be aware of the meaning and limitations for this item to be satisfactory. See Attachment One, Terms for more details.)

A3.2.7. Determine if unit member and staff personnel are aware of AFI 14-104 and DOD 5240.1-R as key intelligence oversight authorities.

(Note: This is a non-critical item. Individuals who are not aware will receive remedial training.)