BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-104

23 APRIL 2012

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/A2RP
Supersedes: AFI 14-104, 16 April 2007

Certified by: AF/A2Z
(Mr. Joseph D. Yount)
Pages: 30

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.* This publication states the requirements for United States Air Force intelligence oversight activities. In this publication, the term intelligence refers to intelligence and counterintelligence units, activities, etc. It describes mandatory intelligence oversight-associated training requirements for Air Force components that conduct intelligence activities. It also details how to identify, investigate, and report in the event of possible violations. This publication does not apply to criminal investigative activities. For purposes of this publication, the National Guard Bureau is a MAJCOM. This instruction applies to all Air Force (USAF), Air Force Reserve (USAFR) 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 and Host Nation employees engaged in or performing intelligence-related activities as provided for in paragraph 2. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/afrims/afrims/afrims/rims.cfm/. Send recommended changes using the AF Form 847, *Recommendation for Change of Publication* to AF/A2 Policy workflow via NIPR or SIPRnet. This publication may be supplemented at any level, but all direct Supplements must be routed through the OPR prior to certification and approval to AF/A2 Policy workflow via NIPR or SIPRnet.

Page 11 Bronze

Page 12 90 days

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 (include 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 conduct or give the appearance ofconducting collection, exploitation or dissemination of 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 IAW paragraph 11.4. Unless otherwise approved, domestic imagery must be withheld from all general access database systems (e.g., Intelink).

9.6. **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. 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 Unmanned Aircraft System (UAS) 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 (CBP), Federal Bureau of Investigations (FBI), US Immigration and Customs Enforcement (ICE), and the US Coast Guard, will control any such data collected.

10. Force Protection.

10.1. 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, 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 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.

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 DoD 5240.1-R, Procedure 2.

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. 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, Judge Advocate General (JAG), 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.

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 for the length of time necessary to transfer it to another DoD entity or government agency to whose function it pertains.

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. 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.

11.2.3.2. 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: