BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-404

3 SEPTEMBER 2019

Intelligence

INTELLIGENCE OVERSIGHT

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/A2/6UZ

Certified by: AF/A2/6U
(Brig Gen James R. Cluff)

Supersedes: AFI 14-104, 5 November 2014

Pages: 16

This publication implements Air Force Policy Directive 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*. It applies to all civilian employees and uniformed members of the Regular Air Force; Air Force Reserve; Air National Guard when performing duty in Title 10 status, and Title 32 status when conducting training for active duty intelligence or intelligence-related activities; as well as to all persons who conduct intelligence or intelligence-related activities on behalf of the Air Force, including contractors when in the terms of their contracts. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility using the Air Force 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 Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include the appointing of the Senior Intelligence Oversight Official, realignment of roles and responsibilities, and reporting requirements when unmasking U.S. persons information contained in intelligence reports.

1. Overview. This guidance contains 59 tiered compliance statements: 45 (T-0); 14 (T-1). This publication provides for the effective conduct of Air Force intelligence activities and intelligence-related activities and the protection of constitutional rights. All lawful means, and with full consideration of the rights of U.S. persons, shall be used to obtain reliable intelligence information to protect the United States and its interests. The Air Force has a solemn obligation, and shall continue in the conduct of its activities, to protect fully the legal rights of all U.S. persons, including freedoms, civil liberties, and privacy rights guaranteed by federal law. Individual intelligence professionals, and their unit commanders, play the most important role in this process.

2. Roles and Responsibilities.

2.1. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6) will:**

2.1.1. Serve as a Defense Intelligence Component Head IAW DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*.

2.1.2. Support all intelligence oversight responsibilities as delegated from the Secretary of the Air Force (SecAF) to the Air Force Intelligence Oversight Officer IAW DoDD 5148.13 *Intelligence Oversight*.

2.1.3. Manage communications with the legislative branch on intelligence oversight issues IAW AFI 90-401, *Air Force Relations with Congress* and in consultation with the DoD Senior Intelligence Oversight Official.

2.1.4. Coordinate with the Air Force Inspector General to develop intelligence oversight inspection requirements for inclusion into AFI 90-201, *The Air Force Inspection System*.

2.2. **Associate Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/AAD2/6) will:**

2.2.1. As appointed by the SecAF, serve as Air Force Intelligence Oversight Official and have access to all component intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments); Air Force Intelligence Oversight Official has direct access to the SecAF on intelligence oversight matters. The Air Force Intelligence Oversight Official assists the SecAF in the administration of intelligence oversight by monitoring the accomplishment of the SecAF's responsibilities in DoDD 5148.13.

2.2.2. Serve as approving official for Air Force intelligence oversight reports submitted to the DoD Senior Intelligence Oversight Official.

2.3. **Air Force Inspector General (SAF/IG) will:**

2.3.1. Ensure all Air Force Questionable Intelligence Activities and Significant/Highly Sensitive Matters are properly identified and investigated in accordance with DoDD 5148.13 **(T-0)**.

2.3.2. In accordance with DoDD 5148.13 and AFI 90-201 ensure Air Force units conducting intelligence and intelligence-related activities are periodically inspected to ensure compliance with all applicable federal law, executive orders, presidential directives, intelligence community directives, and DoD issuances; and in order to:

2.3.2.1. Determine whether any element within their respective jurisdiction is conducting intelligence without an assigned mission **(T-0**).

2.3.2.2. Verify that procedures exist for reporting questionable intelligence activities and significant/highly sensitive matters and that employees are effectively trained on and consistently comply with their intelligence oversight responsibilities **(T-0)**.

2.4. **Secretary of the Air Force, General Counsel (SAF/GC) will provide interpretations of intelligence oversight laws and policy for the Department of the Air Force and advise on Air Force intelligence oversight training and policy.** SAF/GC will review all reports of significant/highly sensitive matters, if time allows, and all reports of questionable intelligence activities.

2.5. **The Judge Advocate General (AF/JA) will provide functional oversight to legal offices responsible for advising Air Force intelligence components.** AF/JA will be responsible for intelligence oversight initial and annual training of members of the Judge Advocate General's Corp with intelligence activity responsibilities. In conjunction with SAF/GC, will review intelligence related policy directives, regulations, and training policies.

2.6. **Major Command (MAJCOM), Numbered Air Force (NAF), Field Operating Agencies (FOA), and Direct Reporting Unit (DRU) Directors of Intelligence/Staff Directors, will:**

2.6.1. Ensure units in the command who conduct intelligence or intelligence-related activities manage an intelligence oversight program IAW DoDD 5148.13 **(T-0)**.

2.6.2. In accordance with DoDD 5148.13, ensure subordinate units administer an intelligence oversight training program, which provides all employees with initial and annual refresher training; content must be tailored to mission requirements **(T-0)**. Senior intelligence officers/staff directors may authorize units within the command to substitute Combat Support Agency intelligence oversight training for personnel assigned to their activities, so long as it is appropriately tailored to the organization's mission.

2.6.3. Report Questionable Intelligence Activities or Significant/Highly Sensitive Matters to the Air Force Intelligence Oversight Official and SAF/IG immediately **(T-1)**.

2.6.4. Appoint in writing, a primary and an alternate intelligence oversight program manager of appropriate grade and experience to manage the intelligence oversight program in the command **(T-1)**.

2.6.5. MAJCOM Directors of Intelligence approve Proper Use Memorandums IAW National System for Geospatial Intelligence Instruction (NSGI) 1806, *Domestic Imagery* **(T-0)**. Refer to **paragraph 4.3.3** for further information on "Proper Use Memorandum."

2.6.6. Establish processes to ensure DoD personnel responsible for drafting contract performance requirements include the condition that the contract requires contractor personnel to comply with appropriate provisions of DoDM 5240.01 **(T-1)**; and report any Questionable Intelligence Activities or Significant/Highly Sensitive Matters to appropriate government officials as identified in the contract **(T-0)**. This requirement is applicable to any contract in which contractor personnel will be conducting or supporting intelligence or intelligence-related activities **(T-0)**.

2.7. **MAJCOM, NAF, FOA, DRU, and Wing Inspectors General (IG) will identify and ensure investigation of reported questionable intelligence activities and/or significant/highly sensitive matters as applicable and immediately notify their associated intelligence oversight program managers and legal counsel (T-1).**

2.8. **MAJCOM, NAF, FOA, and DRU Staff Judge Advocates/Legal Advisors will:**

2.8.1. In coordination with MAJCOM IGs, Commanders, and intelligence oversight program managers, provide legal advice on reported questionable intelligence activities and/or significant/highly sensitive matters **(T-1)**. As needed, consult with SAF/GC on intelligence oversight law and policy **(T-0)**. For matters concerning intelligence oversight policy directives, regulations, or training policies, consult SAF/GC and AF/JA **(T-1)**.

2.8.2. Understand assigned organizational missions and provide counsel concerning intelligence oversight law and policy **(T-1)**.

2.9. **Commanders/Directors of All Air Force Organizations and Units That Conduct Intelligence or Intelligence-Related Activities will:**

2.9.1. Ensure compliance with all intelligence oversight rules when conducting intelligence or intelligence-related activities **(T-0)**.

2.9.2. Appoint intelligence oversight monitors (primary and alternate) of appropriate grade and experience to manage the intelligence oversight program **(T-1).**

2.9.3. Identify and report all questionable intelligence activities and/or significant/highly sensitive matters through their respective chain of command, IG, legal counsel, or intelligence oversight program managers to AF/A2/6 **(T-0)**.

2.9.4. Ensure that no adverse action is taken against any DoD personnel or DoD contractor personnel because they intend to report, report, or reported what they reasonably believe is questionable intelligence activities and/or significant/highly sensitive matters **(T-0)**.

2.9.5. If the unit conducts queries of unevaluated information that is intended to reveal U.S. Person Information (USPI), then establish written procedures to document the basis for conducting such queries **(T-0)**. Units will establish documented procedures for retaining data containing USPI and recording the reason for retaining the data and the authority approving the retention (**T-0)**.

2.9.6. In accordance with DoDD 5148.13, administer an intelligence oversight training program, which provides all employees who conduct intelligence or intelligence related activities, with initial and annual refresher content tailored to mission requirements **(T-0).** Initial training will be conducted within 60 days of assignment **(T-1)**. Intelligence oversight monitors and/or unit training managers will document assigned personnel's intelligence oversight training **(T-1)**.

2.9.7. In accordance with AFI 90-201, annually inspect intelligence oversight programs for compliance **(T-1)**. AF-assigned units will use the Headquarter Air Force Intelligence Oversight self-assessment checklist available within the Management Internal Control Tool **(T-1)**.

2.10. **Intelligence Oversight Monitors will:**

2.10.1. Periodically review unit's produced intelligence products for compliance with applicable standards **(T-0)**.

2.10.2. Administer an intelligence oversight training program that is tailored to mission requirements and provides initial and annual refresher intelligence oversight training to all employees **(T-0)**.

2.10.3. Conduct periodic comprehensive reviews of all intelligence and intelligence-related activities in their unit to verify compliance with federal law, executive orders, Presidential directives, Intelligence Community Directives and DoD issuances; report significant findings to the Air Force SIOO **(T-0)**.

2.10.4. Assist the commander in the administration of intelligence oversight by monitoring the accomplishmennts of the responsibilities in DoDD 5148.13 **(T-0)**.

2.11. **All Airmen Who Conduct Intelligence and Intelligence-Related Activities for the Air Force, and Any Person Who Conducts Intelligence and Intelligence-Related Activities on Behalf of the Air Force will:**

2.11.1. Conduct all assigned intelligence and/or intelligence-related activities IAW all applicable laws and policies **(T-0)**.

2.11.2. Report Questionable Intelligence Activities or Significant/Highly Sensitive Matters to their chain of command or supervision immediately **(T-0)**. If it is not practical to report Questionable Intelligence Activities and/or Significant/Highly Sensitive Matters to the chain of command or supervision, report to any Air Force legal counsel or IG; the General Counsel for DoD; the DoD Senior Intelligence Oversight Official; the Joint Staff IG or intelligence oversight officer; the Legal Counsel to the Chairman of the Joint Chiefs of Staff; the IG DoD; or the Intelligence Community IG **(T-0)**.

3. Identifying, Investigating and Reporting Questionable Intelligence Activities and/Or Significant/Highly Sensitive Matters.

3.1. Commanders shall investigate Questionable Intelligence Activities and/or Significant/Highly Sensitive Matters using procedures for commander-directed investigations IAW AFI 90-301, *Inspector General Complaints Resolutions* **(T-0).**

3.2. MAJCOM, FOA, or DRU intelligence oversight program managers must submit quarterly inputs to the AF/A2/6 intelligence oversight program manager **(T-0)**. The AF/A2/6 intelligence oversight program manager consolidates all inputs into a single Air Force report after coordinating with SAF/GC and SAF/IG. The Air Force Intelligence Oversight Official provides the quarterly report to the DoD Senior Intelligence Oversight Official.

3.3. Air Force personnel assigned to non-Air Force organizations who report Questionable Intelligence Activities or Significant/Highly Sensitive Matters to their duty organization are encouraged to report to Air Force Intelligence Oversight Official or their Air Force Element commander for reporting to the Air Force Intelligence Oversight Official. The Air Force Intelligence Oversight Official will not report Questionable Intelligence Activities or Significant/Highly Sensitive Matters to the DoD Senior Intelligence Oversight Official.

4. Intelligence Oversight Procedural Guidance.

4.1. DoDM 5240.01 and DoD 5240.1-R establish procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the privacy and civil liberties of U.S. persons. At the same time, DoD will provide timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents.

4.2. DoDM 5240.01 requires Defense Intelligence Component Head (or delegee) approval prior to conducting certain activities. Refer to **Attachment 2** for a listing of the Air Force intelligence oversight approval authorities.

4.3. Domestic Imagery: All Air Force requests and/or taskings for overhead domestic imagery from the National Geospational Agency (NGA) will be IAW NSGI 1806. Organizations that make Air Force requests for domestic imagery to support Counter Intelligence or Foreign Intelligence missions will have their servicing legal office conduct a legal review and if required, get a proper use memorandum approved **(T-0)**. Proper Use Memorandums are not needed for domestic imagery from the NGA for testing, training, or exercise use.

4.3.1. Unmanned Aircraft Systems activities: Air Force personnel who use unmanned aircraft systems during missions to collect, retain and disseminate data and/or imagery must do so IAW the guidance in this instruction and in DoDM 5240.01. Domestic Air Force Unmanned Aircraft Systems flights conducting intelligence or intelligence-related activities require a proper use memorandum. All domestic Air Force Unmanned Aircraft Systems flights follow applicable procedures outlined in Air Force Manual 11-502, *Small Unmanned Aircraft Systems*, and the Secretary of Defense memorandum, *Guidance for the Domestic Use of Unmanned Aircraft Systems in US National Airspace* [**https://media.defense.gov/2018/Nov/05/2002059511/-1/-1/1/GUIDANCE-FOR-THE-DOMESTIC-USE-OF-UNMANNED-AIRCRAFT-SYSTEMS-IN-US-NATIONAL-AIRSPACE.PDF**].

4.3.2. Manned weapon systems activities: Air Force units operating aircraft with sensors that are used for intelligence or intelligence related purposes must comply with DoDM 5240.01 **(T-0)**. This does not apply to sensors where their primary function is to provide immediate-use targeting data. Organizations which store dometic imagery will not retrieve the imagery by reference to U.S. Persons **(T-0)**. Units will have a current Proper Use Memorandum on file with their MAJCOM **(T-1)**.

4.3.3. Proper Use Memorandums: Organizations that operate sensors that collect domestic imagery must have an approved MAJCOM PUM before collection **(T-0)**. Organizations that operate sensors that collect domestic imagery for combatant commands must have that combatant command's approved proper use memorandums. Tactical Satellites are considered airborne platforms and so approval authority does not reside with NGA. MAJCOM and FOA Directors of Intelligence/Staff Directors may approve requests, after legal review at the MAJCOM/FOA level. In the event of an emergency or crisis where U.S. Northern Command is designated as lead DoD Operational Authority, all related requests for domestic imagery from airborne or DoD satellite platforms must be coordinated with U.S. Northern Command to ensure compliance with proper use provisions **(T-0)**. Air Force organizations will use MAJCOM-developed templates **(T-1)**.

4.4. Comply with **Attachment 3** when unmasking identities of U.S. persons in disseminated intelligence reports **(T-0)**.

VERALINN JAMIESON, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
Reconnaissance & Cyber Effects Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*, 11 July 2019

AFI 90-201, *The Air Force Inspection System*, 20 November 2018

AFI 90-301, *Inspector General Complaints Resolutions, 27 August 2015*

AFI 90-401, *Air Force Relations with Congress*, 14 June 2012

AFMAN 11-502, *Small Unmanned Aircraft Systems*, 18 July 2019

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFMAN 33-363, *Management of Records*, 31 May 2015

DoDD 5148.13, *Intelligence Oversight*, April 26, 2017

DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, August 8, 2016

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

Foreign Intelligence Surveillance Act (FISA) of 1978, as amended, Title 50 United States Code Sections 1801, et seq.

ICD 112, *Congressional Notification, Annex A, Dissemination of Congressional Identity Information*, 19 January 2017

ICPG 107.1, *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*, 11 January 2018 [**https://www.dni.gov/files/documents/ICPG/ICPG-107.1.pdf**]

NSGI 1806, *Domestic Imagery*, 15 March 2019 [**https://intelshare.intelink.gov/sites/a2/programs/activities/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/a2/programs/activities/Policy/NSGI%201806_15MAR2019_FOUO.pdf&action=default**.]

Secretary of Defense memorandum, Guidance for the Domestic Use of Unmanned Aircraft Systems in US National Airspace, August 18, 2018 [**https://media.defense.gov/2018/Nov/05/2002059511/-1/-1/1/GUIDANCE-FOR-THE-DOMESTIC-USE-OF-UNMANNED-AIRCRAFT-SYSTEMS-IN-US-NATIONAL-AIRSPACE.PDF**].

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 9 September 2009

Abbreviations and Acronyms

AF—Air Force

AF/A2/6—Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

CC—Commander

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

FOA—Field Operating Agency

IAW—In Accordance With

ICON—Investigations, Collections, Operations Nexus Center

IG—Inspector General

MAJCOM—Major Command

NAF—Numbered Air Force

NGA—National Geospational Agency

SAF/GC—Secretary of the Air Force General Counsel

SAF/IG—Secretary of the Air Force Inspector General

SecAF—Secretary of the Air Force

U.S.—United States

USPI—United States Person Information

Terms

Collection—Information is collected when it is received by a Defense Intelligence component, whether or not it is retained by the component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the component. Collected information does not include: Information that only momentarily passes through a computer system of the component; Information on the Internet or in an electronic forum or repository outside the component that is simply viewed or accessed by a component employee but is not copied, saved, supplemented, or used in some manner; Information disseminated by other components or elements of the Intelligence Community; or Information that is maintained on behalf of another U.S. government agency and to which the component does not have access for intelligence purposes.

Counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorists organizations or activities.

Defense Intelligence Component Head—Senior officials designated by the Secretary of a military department for the foreign intelligence and counterintelligence elements of that Department.

Domestic Imagery—A likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, collected in the area that includes the 50 States, the District of Columbia, and territories and possessions of the U.S. to a 12 nautical mile seaward limit of the land areas.

Exigent Circumstances—Circumstances when there is a reasonable basis to believe that there is imminent danger to a person's life or physical safety or when there are time-critical needs that pose significant risks to important U.S. interests.

Foreign Intelligence—Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

Imagery—A likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means. Imagery does not include ground based or handheld images taken by or on behalf of Air Force intelligence organizations.

Intelligence Activities—Refers to all activities that Air Force intelligence components are authorized to undertake pursuant to AFPD 14-4.

Intelligence—Related Activities—Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.)

Masked—The use of alternate or generic wording in data subject to dissemination that does not permit the reader to ascertain the identity of a U.S. person that appeared in an intelligence report.

Proper Use Memorandum—A memorandum signed annually by an organization’s certifying government official. The imagery collecting 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.

Publicly Available Information—Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public.

Questionable Intelligence Activity—Any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an executive order, Presidential directive, intelligence community directive, or applicable DoD policy governing that activity.

Requesting Entity—An entity of the U.S. government or a state, local, tribal, or territorial government that makes a request that is subject to this policy.

Significant or Highly Sensitive Matters—An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an executive order, presidential directive, intelligence community directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the intelligence community, or otherwise call into question the propriety of intelligence activities. such matters might involve actual or potential: congressional inquiries or investigations; adverse media coverage; impact on foreign relations or foreign partners; or, systemic compromise, loss, or unauthorized disclosure of protected information.

U.S. Persons—Includes: a U.S. citizen; an alien known by the defense intelligence component concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments (a corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a U.S. person). A person or organization in the United States is presumed to be a U.S. person, unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained.

U.S. Person Information (USPI)—Information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. USPI is not limited to any single category of information or technology. Depending on the context, examples of USPI may include: names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address information.

Attachment 2

INTELLIGENCE OVERSIGHT APPROVAL AUTHORITIES

Figure A2.1. Intelligence Oversight Approval Authorities.

Intelligence Oversight Approval Authorities					
Procedure #	Item #	Defense Intelligence Component Head	Single Delegee	Multiple Delegees	Reference: DoDM 5240.01, Para.
Procedure 2, Collection	Approve USPI Collection: Threats to Safety	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.2.c.(5).(b)
	Approve USPI Special Circumstance Collection	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1 Note 2	3.2.e
	Approve collecting foreign intelligence concerning U.S. persons within the United States	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Not Authorized	3.2.g.(3).(c)
Procedure 3, Retention	Approve extended Retention of collected USPI (Intentional/incidental/voluntarily-provided)	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Not Authorized	3.3.c.(5).(a)
	Determine the need for enhanced retention safeguards to protect USPI	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.3.g.(1)
	Implementation of enhanced retention safeguards to protect USPI	AF/A2/6 25 AF/CC AFOSI	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.3.g.(2)
Procedure 4, Dissemination	Determine dissemination of USPI to Foreign Governments or International Organizations	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.4.c.(6).(c)
	Determine dissemination of USPI to an entity for the limited purpose of assisting the defense component	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.4.c.(7)
	Assess risk of USPI dissemination for protective purposes	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.4.c.(8)
	Approve dissemination of large amounts of unevaluated USPI	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON	Not Authorized	3.4.d

			Center/CC		
	Approve dissemination of USPI not for foreign intelligence, counter intelligence, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety or protective purpose	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.4.f
Procedure 5, Electronic Surveillance	Notify officials intent to conduct electronic surveillance in emergency situations (requires U.S. Attorney General approval through DoD/GC)	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.5.g.(1)
	Authorize continued electronic surveillance (up to 72 hours) of a foreign person outside U.S. who then enters the U.S. (Emergency situations)	AF/A2/6 25 AF/CC AFOSI/CC	Not Authorized	Not Authorized	3.5.g.(2)
Procedure 6, Concealed Monitoring	Approve concealed monitoring of a U.S. person outside the U.S.	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.6.c.(3)
Procedure 7, Physical Searches	Approve emergency physical searches under Foreign Intelligence Surveillance Act (Defense Intelligence Component head with CI investigation authority only)	AFOSI/CC	ICON Center/CC	Note 1	3.7.c.(3)
Procedure 8, Mail Searches Procedure 8, Mail Cover	Refer to Procedure 7.	AFOSI/CC	ICON Center/CC	Note 1	3.8
Procedure 9, Physical Surveillance	Approve nonconsensual physical surveillance in the U.S.	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.9.c.(1).(c) thru 3.9.c.(1).(d)
	Approve nonconsensual physical surveillance of a U.S. person outside the U.S.	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.9.c.(2).(c)
Procedure 10, Undisclosed Participation in Organizations (UDP)	Approve types of undisclosed participation in organizations: Non-U.S. Persons as Sources of Assistance; Public Forums; Cover Activities; U.S. Person Organizations Outside the United States	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Note 1	3.10.f.(2)

	Approve specific types of sensitive undisclosed participation in organizations (i.e. collection of specific USPI inside the U.S. for counterintelligence purposes)	AF/A2/6 25 AF/CC AFOSI/CC	AF/AA2/6 25 AF/CV ICON Center/CC	Not Authorized	3.10.f.(3)

Note 1: Additional delegations are authorized only by the head of the defense intelligence component. Units requesting additional delegations from the head of the defense intelligence components request them by name, position, grade, or function and must balance the need for speed in decision making with the need for experienced judgment. Additional delegees are typically in the grade of O-6 or equivalent.

Note 2: Delegees must inform the appropriate head of the defense intelligence component through the chain of command when approving action under this rule, in order to allow the Head of the Defense Intelligence Component to report to the DoD Senior Intelligence Oversight Official **(T-0)**.

Attachment 3

REQUESTS FOR IDENTITIES OF U.S. PERSONS IN DISSEMINATED INTELLIGENCE REPORTS

A3.1. This policy applies exclusively to requests from a requesting entity, other than the Air Force: For post-publication release and dissemination of nonpublic U.S. person identity information that was masked in a disseminated Air Force report. This policy does not apply in circumstances where a U.S. person has consented to the dissemination of reporting to, from, or about the U.S. person **(T-0)**.

A3.2. All disseminations must comply with DoDM 5240.01 and: Where applicable, Annex A, *Dissemination of Congressional Identity Information*, of Intelligence Community Directive 112, *Congressional Notification*, or any other applicable provisions of law or policy **(T-0)**.

A3.3. The office receiving the unmasking request shall document (T-0):

A3.3.1. The name, title, organization, and contact information of the person making the request.

A3.3.2. Information that identifies the Air Force report that contains the requested information.

A3.3.3. The name or title of each individual who will receive the U.S. person identity information at the time of release.

A3.3.4. The accountable people under this Paragraph may not be contractors.

A3.3.5. A fact-based justification describing why the unmasked U.S. person identity information is required to carry out the official duties of each person receiving the information.

A3.4. Requests covered by this policy shall be: Approved only by the AF/A2/6, AF/AA2/6, 25AF/CC, or for AFOSI Commander or the ICON Center Commander **(T-0)**.

A3.5. In the event of exigent circumstances or: Where a delay could negatively impact intelligence activities, the information to support the process in **Paragraphs A3.3** and **A3.4** above may be provided verbally. However, within five business days after approval, the requesting entity must provide information needed to comply with **Paragraph A3.3** **(T-0)**. Immediately after that, the Air Force office receiving the request must process the approval under **Paragraph A3.4** **(T-0)**.

A3.6. When an Air Force report contains information that identifies a U.S. person : But that information was originated by a source other that the Air Force, the office receiving the unmasking request shall promptly refer the request to the originating entity and inform the requester **(T-0)**.

A3.7. For any requests made between a general election for President and: The inauguration of such President, inclusive, in addition to the requirements above:

A3.7.1. The requester must assert in writing whether or not the requester has a knowledge or belief that any U.S. person identity information sought is of an individual who is a member of the transition team as identified by the President-elect or Vice President-elect **(T-0)**.

A3.7.2. An Air Force official considering an unmasking request must document any knowledge or reasonable belief that any U.S. person identity information sought by the request is of an individual who is a member of the transition team as identified by the President-elect or Vice President-elect **(T-0)**.

A3.7.3. If such knowledge or belief exists, the unmasking approval shall be subject to the concurrence of the Air Force General Counsel or in the absence of the General Counsel, the Principal Deputy General Counsel **(T-0)**.

A3.7.4. Consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, AF/A2/6, for itself and on behalf of AFOSI, IAW Air Force rules on relations with Congress, and in consultation with the Director of National Intelligence, shall notify the chairmen and ranking minority members of the congressional intelligence committees of any unmasking approval within 14 days **(T-0)**.

A3.8. All requests and approval actions shall be forwarded to: AF/A2/6's appointed Air Force intelligence oversight program manager, who shall retain the request and the information in **Paragraphs A3.3.1** through **A3.3.5** and **A3.7** for not less than five years and then shall archive them as permanent records **(T-0)**.

A3.9. Not later than 1 March of each year: Beginning in 2019, the AF/A2/6 shall submit to the Director of National Intelligence, the congressional intelligence committees, and, through the DoD Senior Intelligence Oversight Official, the Secretary of Defense a report IAW Intelligence Community Policy Guidance 107.1, *Request for Identities of U.S. Persons in Disseminated Intelligence Reports* **(T-0)**. The report will document the following items for the preceding calendar year **(T-0)**:

A3.9.1. The number of requests that the Air Force received, approved, and denied.

A3.9.2. The same information for each requesting entity.