BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE INSTRUCTION 14-404

23 JANUARY 2025

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 (Mr. Arthur C. King)

Supersedes: AFI 14-404, 3 September 2019

Pages: 26

This publication implements Air Force Policy Directive (AFPD) 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; Space Force; Air Force Reserve; Air National Guard when performing duty in status under Title10 United States Code (USC), *Armed Forces*, and status under Title 32 USC, *National Guard*, 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 (AF), including contractors when in the terms of their contracts. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Ensure all records generated as a result of processes prescribed in this publication adhere to 5 USC § 552a, *Records Maintained on Individuals*. Refer recommended changes and questions about this publication to the office of primary responsibility using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*; route DAF 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 office of primary responsibility (OPR) of this publication for coordination prior to certification and approval. Compliance with attachments is mandatory. 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 Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*, Table A10.1, for a description of the authorities associated

with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternately, to the 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 applicability to both the United States Air Force (USAF) and United States Space Force (USSF) as armed forces of the DAF. The update also provides clarifying training requirements language, updated contracting language, a tool to guide determination of intelligence activities, guidance for obtaining clearances for Intelligence Oversight Monitor (IOM) roles, and guidance on dissemination.

1. Overview. This guidance contains 99 tiered compliance statements: 53 **(T-0)**; 34 **(T-1)**; 12 **(T-2)**. This publication assigns responsibilities and establishes policy for the effective conduct of DAF intelligence activities and intelligence-related activities, and the protection of constitutional rights. All lawful means, and with full consideration of the rights of United States (U.S.) persons, shall be used to obtain reliable intelligence information to protect the United States and its interests. The DAF 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. Unit commanders and organization managers with intelligence or intelligence related roles play the most important part in this process.

2. Roles and Responsibilities.

2.1. **Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations (AF/A2/6) and Deputy Chief of Space Operations for Intelligence (SF/S2).** The AF/A2/6 and SF/S2 will:

2.1.1. Serve as a Defense Intelligence Component Head IAW DoDM 5240.01, *DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities*, 27 September 2024. **(T-0)**

2.1.2. Serve as the Head of the Intelligence Community Element (HICE) IAW EO 12333, *United States Intelligence Activities.* The AF/A2/6 is the Head of the Intelligence Community Element (HICE) for the USAF and the SF/S2 is the HICE for the USSF. **(T-0)**

2.1.3. Support all intelligence oversight responsibilities as delegated from the Secretary of the Air Force (SecAF) IAW Department of Defense Directive (DoDD) 5148.13 *Intelligence Oversight*. **(T-0)**

2.1.4. Manage communications with the legislative branch on intelligence oversight issues IAW AFI 90-401, *Relations with Congress*, and in consultation with the DoD Senior Intelligence Oversight Official (SIOO). **(T-1)**

2.1.5. Coordinate with the Air Force Inspector General (IG) to develop intelligence oversight inspection requirements for inclusion into Department of the Air Force Instruction (DAFI) 90-302, *The Inspection System of the Department of the Air Force*. **(T-1)**

2.1.6. Appoint a Service Element Intelligence Oversight Program Manager (IOPM), and other support personnel as required, to support the DAF Intelligence Oversight Official (IOO) and manage the intelligence oversight requirements of the respective headquarters staffs. **(T-1)**

2.1.7. 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). **(T-0)**

2.2. **DAF IOO.** The DAF IOO will:

2.2.1. 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); DAF IOO has direct access to the SecAF on intelligence oversight matters. The DAF IOO assists the SecAF in the administration of intelligence oversight by monitoring the accomplishment of the SecAF's responsibilities in DoDD 5240.01. **(T-0)**

2.2.2. Serve as approving official for DAF intelligence oversight reports submitted to the DoD SIOO. **(T-0)**

2.2.3. Review all waivers and IOPM's by-name IOM recommendations for alternate reviews of intelligence and intelligence-related activity production due to inability of unit IOM to receive appropriate clearances to securely access the materiel. **(T-1)**

2.3. **Secretary of the Air Force Inspector General (SAF/IG).** The SAF/IG will:

2.3.1. Ensure all DAF Questionable Intelligence Activities (QIA) and Significant/Highly Sensitive Matters (S/HSM) are properly identified and investigated in accordance with this directive and DoDD 5148.13. **(T-0)**

2.3.2. Verify that procedures exist for reporting QIA and S/HSM and that employees are effectively trained on and consistently comply with their intelligence oversight responsibilities. **(T-0)**

2.3.3. Ensure DAF units conducting intelligence and intelligence-related activities are inspected for compliance with all applicable federal law, executive orders, presidential directives, intelligence community directives (ICD), and DoD issuances in accordance with DAFI 90-302. Data collected from inspections may be used in official reports as required by DAF, DoD, and congress. **(T-1)**

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

2.3.5. To assist with determination if a specific activity involves intelligence or intelligence-related activities or is research, development, or design for the purpose of future intelligence or intelligence-related activities, the following should be considered:

2.3.5.1. Permission. Focuses on the line of authority relied upon for conducting the activity. An activity is likely an intelligence activity if it relies on an intelligence authority for permission.

2.3.5.2. People. Is the task performed by an intelligence professional or intelligence unit? Under what authority is the person/unit performing the activity? This factor alone is not determinative, as non-intelligence personnel perform intelligence activities if authorized.

2.3.5.3. Purpose. In the military, the purpose of intelligence is typically to provide information on "foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations" to inform commanders decision making. Does the proposed military action require, for example, collection, processing, and integration of this type of information to inform a commander's decisions about a foreign adversary?

2.3.5.4. Pipes. Will the activity result in a product placed on an intelligence directorate's online portal? Will the information acquired during the activity be entered

into intelligence databases for evaluation, or will the finished product (often a report) be entered into intelligence repositories for use by the broader intelligence community (IC)? Does the performance of the activity require access to intelligence databases and resources?

2.3.5.5. Process. Examines how information moves from proposal to fruition. Does the activity require knowledge of intelligence sources or methods? Is it the product of an intelligence planning process? Does the activity require participation of an IC element to acquire, process, or analyze data and/or create products?

2.3.5.6. Platform. Is the activity's required equipment owned or operated by an intelligence unit? If not, will the activity require the use of a non-intelligence platform for an intelligence purpose? For example, the targeting pod on strike aircraft is not an intelligence platform, but it is conceivable that it might be used for an intelligence purpose.

2.3.5.7. Procurement. This factor considers who paid for any equipment needed for the activity. Was it procured using Military Intelligence Program or National Intelligence Program funds?

2.4. **Secretary of the Air Force General Counsel (SAF/GC).** The SAF/GC will:

2.4.1. Provide interpretations of intelligence oversight laws and policy for the DAF and advise DAF IOO on DAF intelligence oversight training and policy. **(T-2)**

2.4.2. Provide advice to the DAF IOPM on reports, investigations, and corrective actions related to QIAs and S/HSMs. **(T-2)**

2.4.3. In conjunction with the DAF IOPM, review quarterly intelligence oversight reports before they are submitted to the DoD SIOO. **(T-2)**

2.4.4. Coordinate with the DAF IOPM on the issuance of guidance to the DAF Components implementing intelligence oversight aspects of E.O. 12333, and E.O. 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board*, as amended. **(T-2)**

2.4.5. Consult with the DAF IOO and DAF IOPM regarding any allegation questioning the legality or propriety of DoD intelligence and intelligence-related activities, or where a reasonable person would believe that the intelligence or intelligence-related activity may be contrary to federal law, E.O.s, presidential directives, ICDs, DoD issuances, and Air Force standards. **(T-2)**

2.4.6. Coordinate with DAF IOPM and DAF IOO on QIA and S/HSM reports to DoD SIOO. **(T-2)**

2.4.7. Provide advice regarding the resolution of disagreement between DAF Components pertaining to investigative authority or jurisdiction for intelligence oversight investigations. **(T-2)**

2.4.8. Review the results of all QIA and S/HSM investigations before the incident is closed in the DAF quarterly intelligence oversight report. **(T-1)**

2.5. **The Air Force Judge Advocate General (AF/JA).** The AF/JA will:

2.5.1. Provide functional oversight to legal offices responsible for advising DAF intelligence components and provide appropriate intelligence law and policy instruction. **(T-1)**

2.5.2. Provide intelligence oversight initial and annual training of members of the Judge Advocate General's Corp with intelligence activity responsibilities. **(T-0)**

2.5.3. Provide interpretations of intelligence oversight laws and policies for the DAF and advice the DAF IOO on DAF intelligence oversight training and policy. **(T-2)**

2.5.4. Review intelligence related policy directives, regulations, and training policies. **(T-1)**

2.5.5. Provide legal advice to the SecAF, Chief of Staff of the Air Force, Chief of Space Operations, DAF SIOO, Service Element IOPMs, and other members of the DAF. **(T-1)**

2.5.6. Consult with the DAF IOO and DAF IOPM regarding any allegation questioning the legality or propriety of DAF intelligence and intelligence-related activities, or where a reasonable person would believe that the intelligence or intelligence-related activity may be contrary to federal law, E.O.s, presidential directives, ICDs, DoD issuances, and Air Force standards. **(T-2)**

2.5.7. Provide advice regarding the resolution of disagreement between DAF Components pertaining to investigative authority or jurisdiction for intelligence oversight investigations. **(T-2)**

2.6. **Service Element Intelligence Oversight Program Manager (IOPM).** The Service Element IOPM will:

2.6.1. Assist the DAF IOO in the administration of intelligence oversight by monitoring the accomplishment of the SecAF's responsibilities IAW DoDD 5240.01 and DoDD 5148.13. **(T-0)**

2.6.2. Review all waivers and provide by-name IOM recommendation for alternate reviews of intelligence and intelligence-related activity production due to inability of unit IOM to receive appropriate clearances to securely access the material. **(T-1)**

2.6.3. 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). **(T-0)**

2.6.4. Collaborate with AF/JA, SAF/GC and SAF/IG to administer and implement the DAF IO program. **(T-1)**

2.6.5. Coordinate with AF/JA, SAF/GC and SAF/IG to consolidate all IO reports inputs into a single DAF report for approval by the DAF IOO. **(T-1)**

2.6.6. Once approved by the DAF IOO, will provide the quarterly report to the DoD SIOO. **(T-1)**

2.6.7. Advise and assist major command (MAJCOM), field command (FLDCOM), numbered air force (NAF), field operating agencies (FOA), deltas, and direct reporting unit (DRU) directors of intelligence/staff directors in interpreting and executing the DAF IO program. **(T-1)**

2.6.8. On a quarterly basis, provide an intelligence oversight report on behalf of the DAF to the DoD SIOO IAW DoDD 5148.13 and **Section 4** of this issuance. **(T-0)**

2.6.9. The DAF IOPM will maintain baseline intelligence oversight training that is accessible force-wide and will assist IOMs in producing specific and tailored training to meet unit requirements. **(T-1)**

2.7. **MAJCOM, FLDCOM, SCC, NAF, FOA, Delta, Wing, DRU Directors of Intelligence/Staff Directors.** The MAJCOM, FLDCOM, SCC, NAF, FOA, Delta, Wing and DRU directors of intelligence/staff directors will:

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

2.7.2. 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)**

2.7.2.1. Within the command, units are authorized but not required to substitute combat support agency-provided intelligence oversight training for personnel assigned to their activities, as long as it is appropriately tailored to the organization's mission. For example, if a unit is assigned to National Security Agency (NSA), they are authorized to use NSA's IO training in lieu of creating their own training, as long as the NSA training is appropriately tailored to the organizations mission. **(T-2)**

2.7.3. Report QIA or S/HSM to the DAF IOO and SAF/IG immediately. Reporting will not be delayed or postponed pending an investigation, command inquiry, or legal proceeding IAW DoDD 5148.13. **(T-0)**

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

2.7.5. Approve proper use memorandums (PUMs) IAW National System for Geospatial Intelligence Instruction (NSGI) 1806, *Domestic Imagery*. **(T-0)**

2.7.6. Coordinate with subordinate units to ensure regular and accurate reporting of QIA and/or S/HSM. **(T-0)**

2.7.7. Establish processes to ensure that personnel within their organization coordinate with appropriate contracting officers/activities and ensure that contracts under which contractor personnel will be conducting intelligence and intelligence-related activities or supporting those efforts under DAF or DoD authorities include requirements for contractor personnel to:

2.7.7.1. Comply with appropriate provisions of DoDM 5240.01. **(T-1)**

2.7.7.2. Report any QIA or S/HSM to appropriate government officials as identified in the contract. **(T-0)**

2.7.8. In coordination with the supporting contracting activity, ensure contracts for intelligence and intelligence-related activities include the following provision as a performance requirement:

2.7.8.1. Contractors who conduct or support intelligence or intelligence-related activities will complete the customer-provided intelligence oversight training as required by customer requirements and will report any QIA, S/HSM, and/or federal crimes IAW procedures established in DoDD 5148.13, *Intelligence Oversight*, and this DAFI. **(T-0)**

2.7.8.2. For contracts involving cryptographic matters, reference United States Signal Intelligence Directive (USSID) 18, *Legal Compliance and U.S. Persons Minimization Procedures* in addition to DoDD 5148.13, and this DAFI. **(T-0)**

2.7.9. Conduct continual evaluation to maintain program oversight and identify gaps or deficiencies in existing policy, guidance, training, and resources. Participate in the continual evaluation processes by monitoring data (e.g., Management Internal Control Toolset (MICT) Self-Assessment Checklists (SAC), trend analysis, and any other existing functional processes). Utilize the MICT SAC to assess and prioritize higher headquarters' requirements and document self-identified, non-compliant observations with corrective actions plans IAW DAFI 90-302. **(T-1)**

2.8. **MAJCOM, FLDCOM, SCC, NAF, FOA, DRU, Delta, and Wing Inspectors General (IG).** The MAJCOM, FLDCOM, SCC, NAF, FOA, DRU, Delta, and Wing IGs will identify and ensure investigation of reported QIA and/or S/HSM as applicable and immediately notify their associated intelligence oversight program managers and legal counsel in accordance with DoDD 5148.13. **(T-0)**

2.9. **MAJCOM, FLDCOM, SCC, NAF, FOA, Delta, Wing, and DRU Staff Judge Advocates/Legal Advisors.** The MAJCOM, FLDCOM, SCC, NAF, FOA, Delta, Wing, and DRU Staff Judge Advocates/Legal Advisors will:

2.9.1. Provide legal advice on reported QIA and/or S/HSM to MAJCOM/FLDCOM IGs, commanders, IOPMs, and IOMs. **(T-2)**

2.9.2. As needed, consult with their technical legal chain on intelligence oversight law, policy, directives, and regulations. **(T-1)**

2.9.3. For matters concerning Judge Advocate intelligence oversight policy directives, regulations, or training, consult AF/JA. **(T-1)**

2.9.4. Understand assigned organizational missions and provide counsel concerning intelligence oversight law and policy. **(T-2)**

2.10. **Commanders/Directors of all DAF organizations and units that conduct intelligence or intelligence-related activities.** The commanders/directors of all DAF organizations and units that conduct intelligence or intelligence-related activities will:

2.10.1. Establish an intelligence oversight program to ensure all intelligence or intelligence-related activities are conducted in accordance with federal law, executive orders, presidential directives, intelligence community directives, and DoD and DAF issuances. **(T-0)**

2.10.2. Ensure during the drafting phase of performance requirements that all contracts which will require contractor personnel to conduct or support intelligence or intelligence-related activities will include the following statement as a performance requirement:

2.10.2.1. Contractors who conduct or support intelligence or intelligence-related activities will complete the customer-provided intelligence oversight training as required by customer requirements and will report any QIA, S/HSM, and/or federal crimes IAW procedures established in DoDD 5148.13, and this DAFI. **(T-0)**

2.10.2.2. For contracts involving cryptographic matters, reference USSID 18, in addition to DoDD 5148.13, and this DAFI. **(T-0)**

2.10.3. Appoint IOMs (primary and alternate) of appropriate grade, clearance levels, and experience to manage the intelligence oversight program. **(T-1)**

2.10.4. Identify and report all QIA and/or S/HSM through their respective chain of command, IG, legal counsel, or IOPMs to AF/A2/6 or SF/S2. National Guard members, while in duty status under Title 32 USC, *National Guard*, will report QIA and S/HSM to the National Guard Bureau (NGB) SIOO and NGB IG. All QIAs and S/HSMs will be reported immediately. Reporting will not be delayed or postponed pending an investigation, command inquiry, or legal proceeding. **(T-0)**

2.10.5. Ensure that no adverse action is taken against any DoD personnel or DoD contractor personnel solely because they intend to report or reported what they reasonably believe is a QIA and/or S/HSM. **(T-0)**

2.10.6. Establish written procedures to document the basis for conducting queries of unevaluated information that is intended to reveal U.S. person information (USPI). 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)**

2.10.7. In accordance with DoDD 5148.13, oversee organization's or unit's 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)**

2.10.7.1. Initial training will be conducted within 60 days of assignment (or 90 days for Air National Guard personnel in status under Title 32 USC). **(T-1)**

2.10.7.2. Intelligence oversight monitors and/or unit training managers will document assigned personnel's intelligence oversight training. **(T-1)**

2.10.8. In accordance with DAFI 90-302, annually inspect intelligence oversight programs for compliance. DAF-assigned units will use the DAF Intelligence Oversight self-assessment checklist available within the Management Internal Control Tool. **(T-1)**

2.10.9. In the event that no unit IOM can receive secure access to all unit intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments), the commander will submit a waiver requesting an appropriately cleared IOM complete the periodic comprehensive reviews of all intelligence and intelligence-related activities within the aforementioned named programs to verify compliance with federal law, executive orders, presidential directives, ICDs and DoD issuances; report significant findings to the DAF IOO. **(T-0)**

2.10.10. Establish and review organization's or unit's dissemination mitigation procedures for intelligence production in the event of need for recall or update IAW Intelligence

Community Policy Memorandum (ICPM) 200(01) *Intelligence Community Standards and Procedures for Revised and Recalled Intelligence Products.* **(T-0)**

2.10.10.1. Unit mitigation procedures will include revising or recalling a report for administrative, substantive or legal reasons to include, but not limited to, recalling a report that used material pursuant to 50 USC § 1801 et seq, *War and National Defense* (Foreign Intelligence Surveillance Act (FISA) of 1978) that has been recalled. **(T-0)**

2.10.10.2. Unit mitigation procedures will include standards for regular review and update of unit owned intelligence databases, share folders or repositories to update revised and/or remove recalled reporting from other agencies in order to reduce further dissemination or use of that reporting. **(T-1)**

2.11. **Intelligence Oversight Monitors (IOMs).** The IOMs will:

2.11.1. Periodically review unit's produced intelligence products for compliance with applicable standards. **(T-1)**

2.11.2. Administer an intelligence oversight training program that is tailored to mission requirements and provides initial and annual refresher intelligence oversight training to all employees. IOMs are authorized, but not required, to substitute combat support agency provided intelligence oversight training for personnel assigned to their activities, so long as it is appropriately tailored to the organization's mission. For example, if a unit is assigned to NSA they are authorized to use NSA's IO training in lieu of creating their own training, so long as the NSA training is appropriately tailored to the organizations mission. **(T-1)**

2.11.3. Conduct periodic comprehensive reviews of all intelligence and intelligence-related activities in their unit to verify compliance with federal law, executive orders, presidential directives, ICDs and DoD issuances; report significant findings to the DAF IOO. **(T-1)**

2.11.4. Have access to all unit intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments). **(T-1)**

2.11.5. In the event access approval cannot be granted to the IOM, IOM will request a waiver for an appropriately cleared IOM to complete the periodic comprehensive reviews of all intelligence and intelligence-related activities within the aforementioned named programs to verify compliance with federal law, executive orders, presidential directives, ICDs and DoD issuances; report significant findings to the DAF IOO. **(T-0)**

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

2.11.7. Provide quarterly intelligence oversight report inputs to the IOPM IAW DoDD 5148.13. **(T-0)**

2.12. **Any person, military, civilian, or contracted personnel, who conducts intelligence and intelligence-related activities on behalf of the DAF.** Any person, military, civilian, or contracted personnel, who conducts intelligence and intelligence-related activities on behalf of the DAF will:

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

2.12.2. Complete IO annual training tailored to their mission and report completion of training to their unit IOM. **(T-0)**

2.12.3. Report QIA or S/HSM to their chain of command or supervision immediately. If it is not practical to report QIA or S/HSM to the chain of command or supervision, report to any DAF legal counsel or IG; NGB SIOO, GC, or IG for the National Guard; the General Counsel for DoD; the DoD Senior SIOO; the Joint Staff IG or intelligence oversight official; the Legal Counsel to the Chairman of the Joint Chiefs of Staff; the IG DoD; or the IC IG. **(T-0)**

3. Identifying, Investigating, and Reporting QIA and/or S/HSM.

3.1. **Identifying.**

3.1.1. DAF personnel must identify and immediately report all potential and confirmed QIA and/or S/HSM through their respective chain of command, IG, legal counsel, or IOPMs to AF/A2/6 **(T-0).** National Guard, while in duty status under Title 32 USC, will report QIA and S/HSM to the National Guard Bureau SIOO and NGB-IG-IO. **(T-0)**

3.1.2. If an inspection conducted IAW DAFI 90-302 identifies a QIA or S/HSM, the matter will be reported and investigated IAW paragraphs **3.2 through 3.3** of this instruction. **(T-0)**

3.1.3. DAF personnel responsible for drafting the performance requirements (statement of work) for any contract under which contractor personnel will be conducting intelligence or intelligence-related activities or supporting those efforts under DoD or DAF authorities shall ensure that the contract requires contractor personnel to report any QIA or S/HSM to appropriate government officials identified in the contract. Officials to whom any such report is made should proceed in accordance with **paragraph 3.1.1**. **(T-0)**

3.2. **Investigating.**

3.2.1. Commanders shall appoint an Inquiry Official to investigate all reports of QIAs and/or S/HSM to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies. At a minimum, investigations will require a written Report of Investigation (ROI) that includes a description of the incident and a determination of whether the allegation was substantiated. If the allegation is substantiated, the ROI will include findings of fact, assessment of the cause, the recommended remedial action to prevent reoccurrence. Commanders will refer all ROIs to the corresponding DoD component IG for further investigation or other action under an appropriate authority as determined by the DoD component head. **(T-1)**

3.2.2. Commanders will utilize the general procedures for a Commander Directed Investigation (CDI) IAW DAFMAN 1-101, as appropriate, to ensure the report contains sufficient information to satisfy the investigative requirements under DoDD 5148.13. **(T-0)**

3.3. **Reporting.**

3.3.1. Commanders will report all potential QIA or S/HSM to the DAF IOO and SAF/IG immediately. IAW DoDD 5148.13, upon appointment of an Inquiry Official, commanders/directors will complete ROI for the following matters to the DAF IOO, regardless of the outcome of investigation or determination of substantiation. **(T-0)**

3.3.1.1. Potential and confirmed QIA.

3.3.1.2. Potential and confirmed S/HSM.

3.3.1.3. Any potential or confirmed intelligence or intelligence-related activity that has been or will be reported to the U.S. Attorney General, or that must be reported to the U.S. Attorney General as required by law or other directive, including crimes required by E.O. 12333 to be reported to the U.S. Attorney General.

3.3.2. DAF Components will notify the DAF IOO before providing any briefings to any congressional committee, member of congress, or congressional staff concerning intelligence or intelligence-related matters that meet the reporting criteria for QIAs, S/HSMs, or crimes reported to the U.S. Attorney General, unless extenuating circumstances exist. **(T-1)**

3.3.3. Should extenuating circumstances prevent advance notification to the DAF IOO, then the DAF IOO will be updated on the briefing's outcome as soon as possible. The DAF IOO is responsible for notifying the DoD SIOO. **(T-1)**

3.3.4. DAF personnel assigned to non-DAF organizations who report QIA or S/HSM to their duty organization are encouraged to report to the DAF IOPM or their DAF unit commander, who will ensure reporting to the DAF IOPM or DAF IOO. These types of incidents will not be included in the DAF quarterly reports as the incidents will be included in the non-DAF organization’s report.

4. Intelligence Oversight Reporting.

4.1. **Quarterly Reporting Requirements.** MAJCOM, FLDCOMs, SCC, FOA, or DRU IOMs must submit quarterly inputs to the DAF IOPM for intelligence oversight reporting. The reporting template is found in DoDD 5148.13, **figure 1**. **(T-0)**

4.1.1. The DAF IOPM consolidates all inputs into a single DAF report after coordinating with AF/JA, SAF/GC and SAF/IG for approval by the DAF IOO. **(T-1)**

4.1.2. The DAF IOPM will provide the quarterly report to the DoD SIOO. **(T-1)**

5. Intelligence Oversight Procedural Guidance.

5.1. **Privacy and Civil Liberties.** DoDM 5240.01 and DoDD 5240.1-R, *Procedures Governing Activities of DoD Intelligence Components That Affect United States Persons*, 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.

5.2. **Prior Approval.** 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 DAF intelligence oversight approval authorities.

5.3. **Domestic Imagery** . All DAF requests and/or taskings for overhead domestic imagery from the National Geospatial-Intelligence Agency (NGA) will be IAW NSGI 1806. Organizations that make DAF requests for domestic imagery to support counterintelligence or foreign intelligence missions will have their servicing legal office conduct a legal review and if required, get a proper use memorandum (PUM) approved. PUMs are not needed for domestic imagery from the NGA for testing, training, or exercise use. **(T-0)**

5.3.1. Unmanned Aircraft/Spacecraft Systems activities: DAF 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 DAF Unmanned Aircraft Systems flights conducting intelligence or intelligence-related activities require a PUM. All domestic Air Force unmanned aircraft system flights follow applicable procedures outlined in Air Force Manual (AFMAN) 11-502, *Small Unmanned Aircraft Systems*, and the Secretary of Defense memorandum, *Guidance for the Use of Unmanned Aircraft Systems in US National Airspace*, *0*2 November 2023, [**https://www.milsuite.mil/book/groups/dodissuances/pages/memos-and-security-policy-memos**]. **(T-0)**

5.3.2. Manned weapon systems activities: DAF units operating aircraft with sensors that are used for intelligence or intelligence-related purposes must comply with DoDM 5240.01. **(T-0)**

5.3.2.1. This does not apply to sensors where their primary function is to provide immediate use targeting data. Organizations which store domestic imagery will not retrieve the imagery by reference to U.S. Persons. **(T-0)**

5.3.2.2. Units will have a current PUM on file with their MAJCOM/FLDCOM. **(T-1)**

5.3.3. PUMs: Organizations that operate sensors that collect domestic imagery must have an approved MAJCOM/FLDCOM PUM before collection. **(T-0)**

5.3.3.1. Organizations that operate sensors that collect domestic imagery for combatant commands must have that combatant command's approved PUMs. **(T-0)**

5.3.3.2. Service satellites that operate sensors that can collect domestic imagery can be approved for domestic collection by the MAJCOM/FLDCOM/FOA Directors of Intelligence/Staff Directors, after legal review at the MAJCOM/FLDCOM/FOA level. **(T-0)**

5.3.3.3. 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)**

5.3.3.4. Air Force and Space Force organizations will use MAJCOM/FLDCOM or MAJCOM/FLDCOM equivalent-developed templates. **(T-1)**

5.4. **Commercially Available Information (CAI) and Publicly Available Information (PAI)** . DAF units that collect, acquire, or use CAI or PAI for intelligence or intelligence-related purposes must comply with DoDM 5240.01, the Director of National Intelligence, *Intelligence Community Policy Framework for Commercially Available Information*, and applicable DoD and DAF CAI and PAI policies. **(T-0)**

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

LEAH G. LAUDERBACK, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
and Reconnaissance and Cyber Effects Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC § 552a, *Records maintained on individuals*

10 USC, *Armed Forces*

32 USC, *National Guard*

50 USC § 1801 et seq, *War and National Defense* (Foreign Intelligence Surveillance Act (FISA) of 1978)

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

AFI 90-401, *Relations with Congress*, 15 September 2020

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

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

DAF Form 847, *Recommendation for Change of Publication*, 15 April 2022

DAFI 90-302, *The Inspection System of the Department of the Air Force*, 15 March 2023

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 Oct 2023

Director of National Intelligence, *Interim Policy Framework for Commercially Available Information*, May 2024

DoDD 5148.13, *Intelligence Oversight*, 26 April 2017

DoDD 5240.1-R, *Procedures Governing Activities of DoD Intelligence Components That Affect United States Persons, Change 2*, 26 April 2017

DoDM 5240.01, *DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities*, 27 September 2024

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

Executive Order 12333, *United States Intelligence Activities*

Executive Order 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board*

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**]

ICPM 200(01) *Intelligence Community Standards and Procedures for Revised and Recalled Intelligence Products*, 27 February 2020

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 November 2012

NSGI 1806, *Domestic Imagery*, 3 March 2022 [**https://intelshare.intelink.gov/sites/geocom/NPS/NSG%20Policies%20%20ACTIVE/NSGI%201806.pdf**.]

Secretary of Defense memorandum, *Guidance for the Use of Unmanned Aircraft Systems in US National Airspace,* 02 November 2023 [**https://www.milsuite.mil/book/groups/dodissuances/pages/memos-and-security-policy-memos**].

USSID 18, *Legal Compliance and U.S. Persons Minimization Procedure*

Prescribed Forms

None.

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*, 15 April 2022

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

CAI—Commercially Available Information

CC—Commander

CDI—Commander Directed Investigation

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

FISA—Foreign Intelligence Surveillance Act

FLDCOM—Field Command

FOA—Field Operating Agency

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directive

IOM—Intelligence Oversight Monitor

IOO—Intelligence Oversight Official

IOPM—Intelligence Oversight Program Manager

IG—Inspector General

MAJCOM—Major Command

NAF—Numbered Air Force

NGA—National Geospatial-Intelligence Agency

NGB—National Guard Bureau

NSA—National Security Agency

NSGI—National System for Geospatial Intelligence Instruction

OPR—Office of Primary Responsibility

PAI—Publicly Available Information

PUM—Proper Use Memorandum

QIA—Questionable Intelligence Activity

S/HSM—Significant or Highly Sensitive Matter

SecAF—Secretary of the Air Force

SIOO—Senior Intelligence Oversight Official

U.S.—United States

USAF—United States Air Force

USC—United States Code

USSID—United States Signal Intelligence Directive

USPI—United States Person

USPI—United States Person Information

USSF—United States Space Force

Office Symbols

16 AF/CC—Commander, 16th Air Force

16 AF/CV—Vice Commander, 16th Air Force

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

AF/AA2/6—Associate Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations

AF/A2/6UZ—Sensitive Activities and Special Security Programs

AF/JA—Air Force Judge Advocate General

AFOSI/CC—Commander, Air Force Office of Special Investigations

SAF/GC—Secretary of the Air Force General Counsel

SAF/IG—Secretary of the Air Force Inspector General

SF/S2—Deputy Chief of Space Operations for Intelligence

SF/S2D—Associate Deputy Chief of Space Operations for Intelligence

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 voluntarily provided 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 IC; 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 DAF intelligence organizations.

Intelligence Activities—Refers to all activities that Air Force intelligence components are authorized to undertake pursuant to AFPD 14-4. See Joint Pub 1-02.

Intelligence-Related Activities—Those activities that are not conducted pursuant to E.O. 12333, but use intelligence funding (e.g., Military Intelligence Program or National Intelligence Program) are rebuttably presumed to be intelligence-related activities. The use of procedures or technology similar to intelligence activities to conduct activities that have separate authorities but are not intelligence activities under E.O. 12333 does not necessarily convert those separate activities into intelligence-related activities.

The term intelligence-related activity also includes those activities that are not conducted pursuant to E.O. 12333, but involve the collection, retention, or analysis of information, and the activities' primary purpose is to: Train personnel to perform intelligence duties or activities. Conduct research, development, testing, and evaluation for the purpose of developing intelligence-specific capabilities; or Conduct intelligence-related sensitive activities, as referred to in DoDD 5143.01. See DoDD 5240.01

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 (PUM)—A memorandum signed annually by an organization's certifying government official. The imagery collecting organization will submit this memorandum annually. It defines their requirements, intended use, and contains a proper use statement that acknowledges their awareness of the legal and policy restrictions regarding domestic imagery.

Publicly Available Information (PAI)—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 (QIA)—Any intelligence or intelligence-related activity that may be unlawful or contrary to an executive order, Presidential directive, ICD, 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 (S/HSM)—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, ICD, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the IC, 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 (USP)—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	AF/AA2/6	Note 1	3.2.c.(5).(b)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Approve USPI Special Circumstance Collection	AF/A2/6	AF/AA2/6	Note 1 Note 2	3.2.e
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Approve collecting foreign intelligence concerning U.S. persons within the United States	AF/A2/6	AF/AA2/6	Not Authorized	3.2.g.(3).(c)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
Procedure 3, Retention	Approve extended Retention of collected USPI (Intentional/incidental/voluntarily provided)	AF/A2/6	AF/AA2/6	Not Authorized	3.3.c.(5).(a)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Determine the need for enhanced retention safeguards to protect USPI	AF/A2/6	AF/AA2/6	Note 1	3.3.g.(1)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Implementation of enhanced retention safeguards to protect USPI	AF/A2/6	AF/AA2/6	Note 1	3.3.g.(2)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		

		AFOSI	AFOSI Center Commander		
Procedure 4, Dissemination	Determine dissemination of USPI to Foreign Governments or International Organizations	AF/A2/6	AF/AA2/6	Note 1	3.4.c.(6).(c)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Determine dissemination of USPI to an entity for the limited purpose of assisting the defense component	AF/A2/6	AF/AA2/6	Note 1	3.4.c.(7)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Assess risk of USPI dissemination for protective purposes	AF/A2/6	AF/AA2/6	Note 1	3.4.c.(8)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Approve dissemination of large amounts of unevaluated USPI	AF/A2/6	AF/AA2/6	Not Authorized	3.4.d
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Approve dissemination of USPI not for foreign intelligence, counterintelligence, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety or protective purpose	AF/A2/6	AF/AA2/6	Note 1	3.4.f
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
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	AF/AA2/6	Note 1	3.5.g.(1)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	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	Not Authorized	Not Authorized	3.5.g.(2)
		SF/S2			
		16 AF/CC			
		AFOSI/CC			

Procedure 6, Concealed Monitoring	Approve concealed monitoring in the U.S. or directed against a U.S. person outside the U.S. (requires GC or legal determination of reasonable expectation of privacy)	AF/A2/6	AF/AA2/6	Note 1	3.6.c.(3)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
Procedure 7, Physical Searches	Approve emergency physical searches under Foreign Intelligence Surveillance Act (Defense Intelligence Component head with CI investigation authority can request U.S. Attorney General approval through DoD/GC)	AFOSI/CC	AFOSI Center Commander	Note 1	3.7.c.(3)
Procedure 8, Mail Searches Procedure 8, Mail Cover	Refer to Procedure 7.	AFOSI/CC	AFOSI Center Commander	Note 1	3.8
Procedure 8, Mail Cover	Inside or outside the U.S.	AF/A2/6	Not Authorized		
		SF/S2			
		16 AF/CC			
		AFOSI/CC			
Procedure 9, Physical Surveillance	Approve nonconsensual physical surveillance in the U.S. (requires coordination with the FBI)	AF/A2/6	AF/AA2/6	Note 1	3.9.c.(1).(c) thru 3.9.c.(1).(d)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	Approve nonconsensual physical surveillance of a U.S. person	AF/A2/6	AF/AA2/6	Note 1	3.9.c.(2).(c)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		

	outside the U.S. (Must be coordinated with CIA)	AFOSI/CC	AFOSI Center Commander		
Procedure 10, Undisclosed Participation in Organizations (UDP) (Fairly limited in scope)	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	AF/AA2/6	Note 1	3.10.f.(2)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
	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	AF/AA2/6	Not Authorized	3.10.f.(3)
		SF/S2	SF/S2D		
		16 AF/CC	16 AF/CV		
		AFOSI/CC	AFOSI Center Commander		
Note 1: Additional delegations are authorized only by the Defense Intelligence Component Head. Units requesting additional delegations from the Defense Intelligence Component Head 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 Defense Intelligence Component Head through the chain of command when approving action under this rule, in order to allow the Defense Intelligence Component Head 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. Applicability. This policy applies exclusively to requests from a requesting entity, other than the DAF. 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. Dissemination. All disseminations must comply with DoDM 5240.01 and, where applicable, Annex A, *Dissemination of Congressional Identity Information*, of ICD 112, *Congressional Notification*, or any other applicable provisions of law or policy. **(T-0)**

A3.3. Unmasking. The office receiving the unmasking request shall document:

A3.3.1. The name, title, organization, and contact information of the person making the request. **(T-0)**

A3.3.2. Information that identifies the DAF report that contains the requested information. **(T-0)**

A3.3.3. The name or title of each individual who will receive the U.S. person identity information at the time of release. **(T-0)**

A3.3.4. The accountable people under this Paragraph may not be contractors. **(T-0)**

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. **(T-0)**

A3.4. Approval. Requests covered by this policy shall be approved only by the Defense Intelligence Component Head (AF/A2/6, SF/S2, 16AF/CC, or AFOSI Commander), their single Delegee (AF/AA2/6, SF/S2D, 16AF/CV, or the AFOSI Center Commander), or additional delegee in writing. Additional delegations are authorized only by the Defense Intelligence Component Head. Units requesting additional delegations from the Defense Intelligence Component Head 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. Waivers for approval authority will be submitted in the form of appointment letter memorandum to the Defense Intelligence Component Head via the DAF IOPM. **(T-0)**

A3.5. Reporting. 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** may be provided verbally. However, within five business days after approval, the requesting entity must provide information needed to comply with **paragraph A3.3**. Immediately after that, the DAF office receiving the request must process the approval under **paragraph A3.4**. **(T-0)**

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

A3.7. Elections . 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. A DAF 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 and SF/S2, for itself and on behalf of AFOSI, IAW DAF 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. Routing. All requests and approval actions shall be forwarded to the appointed DAF 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. Timeline. Not later than 1 March of each year the AF/A2/6 and SF/S2 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 IC Policy Guidance 107.1, *Request for Identities of U.S. Persons in Disseminated Intelligence Reports.* The report will document the number of requests that the DAF received, approved, and denied for each requesting entity for the preceding calendar year. **(T-0)**