BY ORDER OF THE COMMANDER
AIR COMBAT COMMAND

AIR COMBAT COMMAND HANDBOOK
14-404

2 OCTOBER 2020

Intelligence

INTELLIGENCE OVERSIGHT

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: ACC/A23O

Certified by: ACC/A23
(Col Matthew J. Castillo)

Pages: 31

This handbook derives from Air Force Policy Directive 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*, and builds upon guidance found in Air Force Instruction (AFI) 14-404, *Intelligence Oversight*, to provide advisory and informational guidance for all individuals and units in Air Combat Command (ACC)-assigned Regular Air Force (RegAF), Air Force Reserve (AFRC), Air National Guard (ANG), and Department of the AF civilians supporting Air Force (AF) intelligence operational missions at wing-level and below units regarding the execution of Intelligence Oversight. Ensure all records created as a result of processes described in this publication are maintained in accordance with (IAW) AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW the AF Records Disposition Schedule located in the AF Records Information Management System. Refer recommended changes to this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication.

Chapter 1

OVERVIEW

1.1. Purpose. The objective of this handbook is to serve as a comprehensive guide for the effective conduct of Air Force intelligence activities and intelligence-related activities and the protection of constitutional rights, and builds on guidance found in AFI 14-404. Intelligence Oversight (IO) involves a balancing of two fundamental interests: obtaining the intelligence information required to protect national security while protecting individual rights guaranteed by the Constitution and outlined within the laws of the United States. The primary objective of the IO Program is to obtain reliable intelligence information while protecting the legal rights of US Persons (USP) (as articulated in Department of Defense (DoD) Manual 5240.01, *Procedures Governing the Conduct Of DoD Intelligence Activities*), including freedoms, civil liberties, and privacy rights guaranteed by federal law, by ensuring that intelligence personnel at all levels understand IO responsibilities. In short, AFI 14-404 prescribes "what" units must do through directive guidance, while this handbook attempts to inform and advise on "how" to implement an IO program to ensure compliance requirements are met, and more importantly, protect the rights of USPs and information about them (USPI).

1.2. Applicability and Scope. This handbook provides information to all ACC RegAF and gained AFRC and ANG units, staff organizations, to include Numbered Air Force staffs, civilian-contracted organizations and non-intelligence organizations that perform intelligence-related activities that could collect, analyze, process, retain, or disseminate USPI. The handbook will primarily address IO issues at wing and below units, and the term "unit" will be used throughout to indicate wing and below units.

1.3. Background. IO has become a commonly understood term referring to a group of laws, directives, and associated institutional bodies designed to ensure that US intelligence activities are conducted legally and properly, and do not infringe on the rights of USP. For the Air Force, there are five primary governing directives: Executive Order (EO) 12333, *United States Intelligence Activities*, DoD Directive (DoDD) 5240.01, *Intelligence Oversight*, DoD Manual (DoDM) 5240.01, *Procedures Governing the conduct of DoD Intelligence Activities*, DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons,* and AFI 14-404, *Intelligence Oversight.*

1.3.1. Tenets. Air Force intelligence personnel should understand the following central tenets of the Air Force IO program:

1.3.1.1. Scope. The Air Force IO program pertains to all personnel assigned or attached to units or staffs that could collect, analyze, process, retain, or disseminate information on USP. These include active, reserve, guard, civilian, Temporary Duty (TDY) and contractor personnel. Further, the program pertains to any person tasked to perform an intelligence mission regardless of unit of assignment.

1.3.1.2. Permissible Activities. USPI may be collected, retained and disseminated only IAW the procedures in DoDM 5240.01 (Procedures 1-10) and DoD 5240.01-R (Procedures 11-13). In the US, it is not generally within the mission of military intelligence units to collect USPI (this would normally be within the mission of counterintelligence units). As

such, although some USPI may be "publicly available," this does not obviate unit mission/function collection requirements.

1.3.1.3. Collection Techniques. There are very specific procedures and restrictions governing the collection of USPI by methods such as electronic surveillance or physical search or through participation in activities of private organizations (DoDM 5240.01, Procedures 5-10 and DoD 5240.1-R, Procedure 11).

1.3.1.4. Law Enforcement Assistance. There are very specific procedures and restrictions on providing intelligence support to law enforcement agencies (references: AFI 10-801, *Defense Support of Civil Authorities,* DoD 5240.1-R, Procedure 12, and DoD Instruction [DoDI] 3025.21, *Defense Support of Civilian Law Enforcement Agencies*).

1.3.1.5. Questionable Intelligence Activities (QIA). IO is much broader than just collecting, retaining and disseminating USPI. Unit members or staff personnel are required to report QIAs which is defined as "any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including EO 12333, or applicable DoD policy, including DoD 5240.1-R. Unit members or staff personnel are also required to report "Significant or Highly Sensitive Matters" (S/HSMs) (reference: DoDD 5148.13, *Intelligence Oversight,* paragraph 4.1.a.).

1.3.1.6. Reporting a QIA or S/HSM. Personnel assigned to intelligence units or staffs must immediately report any possible IO-associated violations or irregularities (QIAs or S/HSMs) to their supervision, chain of command, IO monitor (IOM), unit Judge Advocate (JA), unit Inspector General (IG), Air Force General Counsel (GC) or IG, or the DoD IG or GC ,or DoD Senior IO Official (SIOO). Use the supervisory chain or chain of command to facilitate such reports, where feasible. Such reports will be expeditiously provided to the IG at the first level at which an IG is assigned who is not associated with the questionable activity. Copies of the report must be sent to the Staff JA and, unless the IG determines such reporting would not be appropriate, senior intelligence officers at the same level (references: DoDD 5148.13, paragraph 4.1.a., AFI 14-404, paragraph 2.9.3.).

1.3.1.7. The Internet. While much of the information posted on the Internet is publicly available information (PAI), PAI may be collected, retained, and disseminated only if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function of the unit or person conducting the intelligence activity. Certain internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation. Intelligence analysts must comply with AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR),* and the *Civil Liberties and Privacy Guidance for Intelligence Community Professionals* requiring disclosure of an individual's intelligence organization and affiliation. This also applies to information found on SIPRnet and JWICS (references: DoDM 5240.01, Procedures 5 &10, and DoD 5240.1-R, Procedure 11).

Chapter 2

INTELLIGENCE OVERSIGHT PROGRAM EXECUTION

2.1. Applying Intelligence Oversight to your unit.

2.1.1. AFI 14-404 and DoDD 5148.13 require units that conduct intelligence or intelligence-related activities to "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." Collection of USPI and its proper retention and dissemination, along with the effective conduct of Air Force intelligence activities and intelligence-related activities and the protection of constitutional rights must be the focus of a unit IO program. All lawful means, and with full consideration of the rights of USP, shall be used to obtain reliable intelligence information to protect the United States and its interests.

2.1.2. What does it mean to "collect" information? Answer: 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. So, if information collected could or does include USPI, then it is an IO matter and your unit must comply with Presidential, DoD, and Air Force directives for the safeguarding and use of USPI, and know how to report QIA and S/HSM. See DoDM 5240.01, Glossary for the definition of "collect."

2.2. Determining Who Requires IO Training in Your Unit.

2.2.1. Once it is clear how IO affects your unit, the next big question is who requires IO training, and who doesn't. As stated in the preamble, the goal of IO is to preserve USP rights and to collect, retain, and disseminate USPI only within the bounds of Federal law. It is important to note that IO requirements follow the activity, not the profession, and that intelligence activities take place within both intelligence (e.g., Distributed Common Ground System units) and non-intelligence units (e.g., a fighter wing). Accordingly, IO training will likely be required for at least some part of every unit. At minimum, the following require IO training within any unit:

2.2.2. All assigned intelligence personnel.

2.2.3. Commanders. In a non-intelligence wing, this typically includes the wing, group and squadron commanders.

2.2.4. Wing Judge Advocate and Wing Inspector General personnel. Wing Inspection Team (WIT) falls under the wing's responsibility and can have a role in any IO issue or concern and therefore require IO training. So, the IOM must ensure WIT personnel receive and maintain their IO training, directly or through other arrangements- but the training and currency must be documented. AF/JA is responsible for IO initial and annual training of members of the Judge Advocate General's Corp with intelligence activity responsibilities.

2.2.5. Air Force Office of Special Investigations (AFOSI). AFOSI special agents receive their initial and annual IO Training through their AFOSI HQ's web site and their regional AFOSI

office IOM tracks completion. So there is no need for wing IOMs to provide or track their training; however, it should be noted that AFOSI does not train SF personnel in IO.

2.2.6. Integrated Defense (ID). IO is also part of the required training for personnel with ID responsibilities IAW AFI 31-101, *Integrated Defense (ID)*, paragraphs 1.5, 1.5.1 and 1.6.21.5. The Integrated Defense Council (IDC) coordinates with AFOSI and the host unit (in-garrison) intelligence to identify training requirements and develop an appropriate Force Protection (FP) threat awareness, which includes IO training. The IO monitors should be involved in this process and coordinate with those necessary to provide and track the initial and refresher IO training for all necessary personnel.

2.2.7. Security Forces (SF) personnel. SF Staff intelligence (S-2) including SF/CC require IO training. IO Monitors should contact their local SF to ensure they are accomplishing the most up to date IO training. This should be part of the training needs captured during the coordination of the IDC, but if not please be aware it is a requirement. The IO Monitors should coordinate tracking of the S-2 team's IO completion dates, or at least be aware of the points of contact (POC) within the S2 team providing and tracking the IO training.

2.2.8. Wing Operations Security (OPSEC). IO training is required for the Wing OPSEC Signature Managers IAW AFI 10-701, *Operations Security (OPSEC)*, paragraph 4.4.6 and Table 4.1. The ACC/A2 IO baseline training is provided online through the AF OPSEC SharePoint site. IO Monitors should contact the Wing OPSEC office for IO completion dates and track their training, or at least be aware of the POCs within the OPSEC office providing and tracking the IO training.

2.2.9. Mission Defense Teams (MDT). IAW ACCMAN 14-402, *Unit Level Intelligence Mission & Responsibilities*, paragraph 6.2, "The SIO, either host unit or tenant as situation dictates, will ensure intelligence support to their local cyber MDT (T-2).' This support can include IO training for members of the MDT to familiarize them with requirements placed on intelligence activities. IOMs should be involved in this process and coordinate with those necessary to provide and track the initial and refresher IO training for all MDT personnel. When providing IO training to MDTs, it is important to remember that while it is helpful for MDT personnel to understand IO requirements and what is permissible under intelligence authorities, IO requirements are applicable only to intelligence activities, which MDTs are typically not authorized to perform (DoDM 5240.01, para 3.1.a.(1)). This means that some units and personnel who receive IO training will not actually be subject to IO requirements. Application of IO requirements to personnel or a unit performing non-intelligence missions or functions should be clearly communicated to those units/personnel after consultation with the IO monitor and the servicing legal office. See ACC Intel support to MDT handbook loaded to SIPR ACC/A2 Unit support "Eagles Nest. Contact ACC/A23O for a link or a copy of the handbook.

2.2.10. Aircrew. Generally aircrew do not require IO training; however, there are exceptions:

2.2.10.1. Any ISR platform whose aircrew/crew control the sensor(s) and might collect on civilian personnel, vehicles or property (includes airborne aircraft and watercraft afloat) must ensure their aircrew and sensor operators receive and maintain IO training.

2.2.10.2. Any platform whose sensor(s) is intended to provide "immediate-use targeting data" (e.g., targeting pod), the aircrew do not normally need IO training. However, if the

imagery is to be used for intelligence purposes, the aircrew will require IO training. Again, this is only true if the targeting pod is going to collect for intel purposes. If they are using the pod for target training or waypoints, it is fine. For instance, they can target a silo on a farm or a factory purely for training purposes without triggering the need for IO training.

2.2.10.3. In addition to the categories above, there may be personnel who need IO training even though they do not occupy one of these positions due to the circumstances in which they are working. Examples of this might include:

2.2.10.3.1. Typical legal uses of domestic imagery are: natural disasters, environmental studies, and exercise, training, testing or navigational purposes. Imagery within the boundaries of a US military training range are authorized, as long as they:

2.2.10.3.1.1. Do not intentionally collect on private facilities or housing areas. Incidental collection is acceptable, meaning the private facilities were not the primary target of collection.

2.2.10.3.1.2. Are not directed at specific USPs.

2.2.10.3.1.3. Are reviewed and approved at the appropriate level.

2.2.10.4. What are the rules for platform sensors over US territory?

2.2.10.4.1. Air Force non-ISR aircraft (e.g., fighters) can fly over the US with its sensors active, but only if not intending to collect on USPs, and as long as it is for training and there is no plan/intent to keep the images.

2.2.10.4.2. Air Force ISR aircraft (e.g., MQ-9, RQ-4, U-2) can fly over the US with its sensors active, but only if they are flying over Proper Use Memorandum (PUM) approved training areas. Typically tactical ISR platforms are restricted to ranges and MOAs, and they cannot fly over public areas, except the RQ-4.

2.2.10.4.3. Additionally, a Defense Intelligence Component may intentionally collect imagery that incidentally contains USPI provided that the collection is not directed at a specific USP; or, if the collection is directed at a specific USP, the collection falls in one of the other categories authorized by DOD 5240.01, para 3.2.c.(12)(a).

2.2.11. If you or your crews/sensor operators think they saw something improper on their pod, sensor feed while on mission, or afterwards during debrief it is thought the crew/sensor operators may have collected on a USP, immediately contact your chain of command or supervisor. They'll work through the legal office and the appropriate higher authority.

2.2.12. Moving Object Tracking. A critical component of Air Force sensor operator training is to prepare crews to conduct missions in deployed locations, including the ability to track mobile objects in both urban and rural settings. ACC personnel are not authorized to record, retain or disseminate data acquired during training missions for the purposes of intelligence exploitation unless otherwise required by law or policy, subject to explicit ACC approval. To enable this training, ACC ISR, Fighter/Bomber, and Remotely Piloted Aircraft (RPA) assets equipped with Electro-Optical/Infrared/Synthetic Aperture Radar/Moving Target Indicator sensors may perform visual reconnaissance of random vehicles on public roadways, within in DoD Small Unmanned Aircraft Systems (SUAS), during training missions under the following conditions:

2.2.12.1. All appropriate activities of this nature are supported by an applicable PUM (see section 2.3 of this handbook).

2.2.12.2. Proper approval authority and other applicable permissions (i.e., Federal Aviation Administration approval for RPA airspace) for the training have been acquired.

2.2.12.3. Commanders are required to take necessary steps to ensure objects captured during these visual reconnaissance training activities are either not recorded or, if recorded, are deleted/erased from the imagery hard drives/sensors of weapon system platforms and or off board media. Information that could lead to identification of a specific US person or his/her identifiably unique features attributable to that specific US person will not be retained for use in simulations or courseware.

2.2.13. What about information rather than imagery or sensor feed? For instance, cyber, signals intelligence (SIGINT), or open source intelligence (OSINT)/PAI.

2.2.13.1. Cyber. Cyber units that provide cybersecurity may require IO training as part of their mission to defend the network by collecting information (i.e. analyzing internet traffic) for threats potentially involving USPI. If you or your analysts are conducting target research, valid targets could appear to be originating from the US. For more information, please refer to USSID SE3000, *SIGINT Mission of USAF Cryptologic Forces*, Annex A.

2.2.13.2. Ensure that you are conducting valid collection at all times as digital communications (usually email) and travel can take place at any time. An individual that you have been lawfully targeting for months could eventually discuss plans to visit people in the US, or be talking with family members that are USPs. These collections would need to cease unless there are extenuating circumstances. For more information, please refer to USSID 3000 Annex A.

2.2.13.3. In your collection you may come into contact with various communications to, from or about corporations. If a corporation is incorporated in the US, you cannot collect on it unless it is determined that it is directed and controlled by a foreign government or governments.

2.2.13.4. When targeting a domain, you may come across a registrant who is in the US. This is a potential incident that needs to be coordinated with IOM and Chain of Command.

2.2.13.5. When targeting a corporation, they might have servers in multiple countries to include the US. Before targeting continues you need to ensure you are targeting the correct selector and not just the name. For more information, please refer to USSID 3000 Annex A.

2.2.14. SIGINT. A phone number that is targeted lawfully all of sudden appears in the US, collection needs to cease, and you need to alert your IO rep and Chain of Command. If this activity took place on NSA systems, the QIA should be reported through NSA's reporting process via the local Intelligence Oversight Officer (IOO). Reporting such activity outside of need-to-know channels could create an additional incident.

2.2.14.1. Any unit or element performing SIGINT/cryptologic functions need to follow USSID 3000, Annex A (USAF SIGINT Intelligence Oversight Program), not service oriented IO. QIAs/incident reporting involving SIGINT must be reported via AFCO/NSA in real time as specified in USSID 3000, Annex A, not via service channels.

2.2.15. OSINT/PAI. To make a definitive determination, we advise discussion with the ACC IO program manager and/or the PUM program manager (links provided in **Attachment 2**), and AFMAN 14-405 or the OSINT/PAI Program Managers.

2.3. PUM requests.

2.3.1. PUM approval resides with MAJCOM A2. For ACC A22M is the PUM authority within ACC and provides annual PUM renewals every April. Special PUM requirements should be addressed with ACC/A2 PUM Manager (links provided in **Attachment 2**).

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

2.3.3. ACC/A2 will provide a timely response to requesting units that include any rules of engagement, if necessary.

2.4. Your IO Training Program.

2.4.1. Annotate and track all IO training for all required personnel within your unit. This includes both initial training (required within 60 days of assignment to the unit), the annual refresher training and pre-deployment training as applicable. Most units find a spreadsheet works well, but there isn't a specific format/tool required for use.

2.4.2. Ensure IO training does not lapse during extended TDYs/deployments. A good practice is to get IO added to the TDY/deployment checklist.

2.4.3. For ANG units: state and regional domestic incident planning may involve your unit. If it does, your aircrew will require IO training. For more information please contact the NGB-J2 IO program manager, or NGB/A2 Unit support, (links provided in **Attachment 2**).

2.4.4. Tailor training to the specific mission of your organization. Training may take many forms, but there are certain minimum requirements to which all organizations must adhere. First, familiarity with the provisions of EO 12333, DoDM 5240.01 and any implementing instructions which apply to your service or agency is required. At a minimum, this entails an understanding of at least DODM 5240.01 and those other procedures that pertain to activities performed by the organization. It should be emphasized in the training that reporting questionable activities is mandatory and that no adverse action may be taken against employees for reporting questionable activities.

2.4.5. ACC/A23O provides the baseline training slide show on the Eagles Nest IO SharePoint Portal (SPP): **https://cs2.eis.af.mil/sites/12024/nest/pages/io.aspx**, but you should add your unit's particulars to the baseline brief to ensure your personnel are trained on the specifics of your Intel/Intel-related mission and where IO issues/questions may come up. Also on the IO SPP are plenty of useful briefings, templates and tools to use in your IO program. Take advantage of them!

2.5. Creating and Maintaining Documentation.

2.5.1. The IOM should create an IO Training roster for his/her area of responsibility with the ability to track both initial and annual training, as well as predeployment IO training completion dates. List all your Intel personnel, affected commanders, aircrew and/or sensor operators (as applicable), IG Intel evaluators, and JA personnel, and anyone else deemed

necessary to receive IO training within your unit. Others that may be added to your training roster may be SF personnel involved in ID/FP, and Wing OPSEC Signature Managers; however, if IO training is being tracked sufficiently within those organizations then you as the IOM need only reference this and be able to the necessary POCs. Coordinate with your orderly room to ensure initial IO training is a requirement listed on the in-processing checklist for all new or transferring personnel, and ensure IO refresher training added to the extended TDY/deployment checklist for accomplishment or at least checked to be sure it will not lapse during an extended TDY/deployment. When the new troop visits you, have them take the initial IO training and add their name and completion date on your tracking roster. Ensure that initial IO training is also listed on required tasks for Initial Qualification Training.

2.5.2. IOM Continuity. People within a unit get reassigned, deployed, retired, or are suddenly unavailable to perform their assigned role. That's why it's imperative to create a continuity book/file/checklist to prevent the loss of corporate knowledge and enable the next person filling in to continue to execute your unit's IO program at a high level (see **Attachment 4**).

Chapter 3

FREQUENTLY ASKED QUESTIONS (FAQS)

3.1. CAF/Standard OSS unit FAQs.

3.1.1. Question: Where does it state in AFI 14-404 that 100% of all those requiring IO training must be trained and current?

3.1.1.1. Answer: While AFI 14-404 does not state "100%", it does say "all". The requirement is clearly stated in the governing DoD publication. AFI 14-404, paragraph 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)." And: DoDD 5148.13: 2.4.c. "Administer an intelligence oversight training program that is tailored to mission requirements and provides initial and annual refresher intelligence oversight training to ***all*** employees."

3.1.2. Are there unique IO requirements for F-35 units? Please advise.

3.1.2.1. Answer: We're not aware of any IO specific requirements to the F-35, or any other 5th-generation units for that matter. There's a lot the MDS/mission set can conceivably collect, but if they are not intending to collect on USPs, and as long as it is for training and there is no plan/intent to keep the images/data we don't think the aircrew require IO training on that basis (i.e., they only need IO training if that platform is being used for an intelligence activity). Of course, any Defense Support of Civil Authorities (DSCA) support obligations could impact that assessment.

3.1.3. Question: I'm the IOM for my squadron as well as the alternate IOM for the Wing. I want to clarify that the self-assessment communicator (SAC) applies to IO programs at both the squadron and wing levels. I'm assuming it does, but I wanted to make sure before I gave my commander a definitive answer.

3.1.3.1. Answer: The newest IO MICT SAC applies to all military Intel units, staff orgs, civilian contracted orgs and non-Intel orgs that perform Intel-related activities that could collect, analyze, process, retain, or disseminate info on USPs. However, there is no need to run the SAC at both the squadron level and wing levels. We generally advise units to execute the SAC at the wing-level, and that the wing IOM gather information from the squadrons to properly assess the IO program across the wing. In the past, we've found units that executed the SAC at both squadron and wing levels resulted in differing and conflicting responses. We understand the units may have multiple GSUs that might make separate assessment tempting, but unless you're directed otherwise we highly advise a single wing-level assessment.

3.2. ISR/DCGS unit FAQs.

3.2.1. Question: Do we need a PUM for this unmanned aircraft system scenario? The intent is for Research and Development, field assessment, operator training for incident responses/maintenance prep and training missions. No intent to collect USPI and all data will

be deleted unless necessary to retain (i.e. base mishap/SF investigation). The Unit prepped a PUM referencing AFMAN 11-502, *Small Unmanned Aircraft Systems*, and stated the purpose is not Foreign Intelligence (FI)/Counter Intelligence (CI) as they are not an Intel collection capable unit. The excerpt states that a PUM is needed for the SUAS that is conducting FI/CI/other intel-related activities. My thought is that a PUM wouldn't be needed based on what Enclosure 2 reads, but I understand the need to cover down intent.

3.2.1.1. Answer: Only if conducting CI/FI is a PUM required. See AFMAN 11-502 for more information.

3.2.2. Question: Seeking opinion on whether our attack squadrons require IO training. The unit launches and recovers the MQ-9 as part of the formal training unit (only performs launch/recovery training). **Note:** My recommendation will be to have an IO program since they operate ISR platforms domestically, but I'm not seeing any written guidance that mandates it for them.

3.2.2.1. Answer: We think your recommendation is the right way to go with this unit. Yes they require training as they are operating an ISR platform over US territory. IAW with the references below, it appears that at the very least their range training activities necessitate awareness of QIA and S/HSMs.

3.2.2.2. AFI 14-404, para 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)."

3.2.2.3. DoDD 5148.13: Section 1, para.1.2.c., "An activity or conduct that qualifies as either a QIA or S/HSM is reportable under Section 4 without waiting for substantiation, completion of an investigation, formal adjudication, or final resolution of the issue." Para. 1.2.d., "Intelligence and intelligence-related activities reportable to the DoD SIOO are not limited to those that concern US persons."

3.2.2.4. DoDD 5148.13: Section 2, para 2.4., "DOD Component Heads Conducting Intelligence Or Intelligence-Related Activities. The DoD Component heads conducting intelligence or intelligence-related activities: c. Administer an intelligence oversight training program that is tailored to mission requirements and provides initial and annual refresher intelligence oversight training to all employees."

3.2.2.5. Responsibilities of DoD personnel and DoD contractor personnel for reporting QIAs and S/HSMs IAW DoDD 5148.13, section 4, paragraph 4.1.a.

3.2.2.6. DoDD 5148.13: Section 4.1. Identification. a. DoD personnel must identify any QIA or S/HSM to their chain of command or supervision immediately. If it is not practical to report a QIA or S/HSM to the chain of command or supervision, reports may be made to the DoD Component legal counsel or IG; the GC DoD; the DoD SIOO; the Joint Staff IG or IO officer; the Legal Counsel to the CJCS; the IG DoD; or the Intelligence Community IG.

3.2.2.7. From the ACC PUM Manager: Both units require IO training if they are operating an MQ with its imaging sensor on - which they had better be for safety of flight. If that sensor is pointed at the ground just once, IO Training is required.

3.3. Cyber Unit FAQs.

3.3.1. Question: What if my unit is functionally aligned to the Joint Forces Headquarters-Cyber AF under 16 AF?

3.3.1.1. Answer: You will follow United States Code and DoDD 5240.01, to include Enclosures 2-7 for IO guidance, not service oriented IO. Any unit or element performing SIGINT/cryptologic functions need to follow USSID 3000, Annex A (USAF SIGINT IO Program), not service oriented IO. ACC doesn't do IO policy for SIGINT. A unit IOM may be service-retained, but they will be doing NSA's brand of IO. The Advanced Distributed Learning System (ADLS) allows training managers to give personnel credit for the annual NSA IO training conducted at AF units.

3.3.1.2. Additionally, all incidents involving SIGINT need to be reported via AFCO/NSA IRT as specified in USSID 3000, Annex A, not via service channels.

3.3.2. Question: I work at NSA, Ft. Meade, MD, in a USAF squadron. Inbound AF personnel complete the ACC IO baseline training while in admin hold awaiting their clearances. Our squadron IO monitor documents the initial training. Once cleared, individuals enter NSA workspaces and receive IO training from NSA. My AF squadron commander interprets AFI 14-404 to say that we must maintain a separate IO program aside from NSA, necessitating redundant overlapping IO training and accountability. Doesn't NSA's IO program count for the AF requirement?

3.3.2.1. Answer: As long as your personnel are doing a NSA mission, they fall under NSA's IO rules and program and you shouldn't have to have a separate AF-oriented IO program. However, since you are already tracking them for their initial AF IO training, it would be a good idea to make a note once they gain access to NSA that they will accomplish their annual and pre-deployment (if necessary) IO Training through the NSA IO Program.

3.3.3. Question: Where can I find information regarding IO and the internet, IP addresses, emails, and Social Media use?

3.3.3.1. Answer: Look in CNGBM 2000.01A, *National Guard Intelligence Activities,* Enclosure H: The Internet and Social Media. We know it's a NGB manual and yours is a RegAF unit, but it has good information on IP addresses, email addresses, URL's and social media use. And there is a lot of good information regarding defining situations.

3.3.3.2. Rule of thumb for emails: An email name does not provide sufficient information to identify an affiliation with a USP; however, persons using a service provider closely affiliated with the US are presumed USP, while the opposite presumption can be made if the provider is not closely affiliated with the US. An inquiry should be made with this rule of thumb as a starting point to better determine if the email address is associated with a USP.

3.3.3.3. Once the decision is made to conduct analysis focused upon specific IP addresses, the "collecting" component is obliged to conduct a reasonable and diligent inquiry to determine whether any of the IP addresses are associated with USP. Rule of thumb for IP addresses: addresses assigned to US-based clients are presumably associated with USP, and addresses assigned to foreign Internet Service Providers (ISPs) presumably are not

associated with USP. Make an inquiry to determine if an IP address is associated with a USP. If unable to reasonably determine if an IP address is associated with a USP, assume it is not a USPI.

3.3.3.3.1. Even if an inquiry reveals that an IP address is assigned to a US service provider, that is not necessarily sufficient information to presume that the address is associated with a USP; however if solid information is obtained subsequently to indicate that an IP address is associated with a USP, then the original presumption is overcome and that IP address must be handled as USP information.

3.3.3.3.2. Some ISPs principally provide service to a US-based clientele. An IP address within a block assigned to such an ISP might merit the presumption that any IP address within that block identifies a USP.

3.3.3.3.3. If a group of IP addresses is known to be assigned to a non-USP (e.g., a foreign corporation), then presume that any given IP address within that block is associated with a non-US person.

3.3.3.3.4. The collecting intelligence component should document the efforts made to determine whether the IP address in question is associated with a USP.

3.3.4. Question: On the ACC wing IG inspection checklist, item 3 it states "include non-intel personnel within the unit" referencing 2.9.1: "Ensure compliance with all intelligence oversight rules when conducting intelligence or intelligence-related activities." We are an ANG unit with MQ-1 mission, and because of this confusing criteria, we were wondering if our commander support staff (CSS) and Communications (COMM) folks also need to complete IO training? Also, we have a SIGINT mission causing some people here to require additional oversight and compliance. Would this be part of our IO program as a whole or an additional oversight program? How would this be inspected and more importantly, run correctly?

3.3.4.1. Answer: This really refers to aircrew and others who might encounter information on USPs in the course of their normal military duties as related to IO, and includes your wing IG and JA as well. CSS and COMM personnel normally do not need IO training because they're not in a position to "collect" USPs information.

3.3.4.2. Your SIGINT personnel typically operate under NSA IO rules and guidelines and get their training from NSA as well- if they are executing a NSA mission. If they are accomplishing an AF mission, then they would receive IO training through the unit like all other Intel within the 119 Wing. Sounds as though they fall under NSA.

3.3.4.3. You could exclude your SIGINT folks from your wing IO program since they follow NSA IO rules and are trained by NSA, but I'd just be sure that you annotate that information in your IO training roster/continuity book.

Chapter 4

SCENARIOS

4.1. CAF Readiness Scenarios.

4.1.1. Typical legal uses of domestic imagery are for: natural disasters, environmental studies, and exercise, training, testing or navigational purposes. Imagery within the boundaries of a US military training range are authorized, with some exceptions per AFI 14-404, para 4.3.

4.1.1.1. Does not include private facilities, privately-owned vehicles, or housing areas.

4.1.1.2. Not directed at specific USPs.

4.1.2. You are working with fighters - How do you make sure IO isn't a problem?

4.1.2.1. Answer: A Defense Intelligence Component may intentionally collect imagery that contains USPI provided that the collection is not directed at a specific US person or, if the collection is directed at a specific USP, the collection falls in one of the other categories authorized by Paragraph 3.2.c (reference: DOD 5240.01, para 3.2.c.(12)(a)).

4.1.3. Your crews think they saw something illegal on their pod - immediately contact your chain of command or supervisor.

4.1.3.1. Answer: They'll work through the legal office and the appropriate higher authority (reference: AFI 14-404 para 2.11.2.).

4.1.4. Can a USAF tactical aircraft (non-ISR) fly over the US with its sensor's active?

4.1.4.1. Answer: Yes, if it is for training and they do not plan to keep the images, and they are not intending to collect on USPs (reference: AFI 14-404, para 4.3.1).

4.1.5. During debrief and reviewing of the "tapes" you think the crew may have collected on a USP. What actions should you take?

4.1.5.1. Answer: Report what you found to your chain of command or your supervisor. (reference: AFI 14-404, para 2.11.2.)

4.1.6. If in the course of your intelligence mission or duties, something doesn't seem right and you think there is an IO issue, what do you do?

4.1.6.1. Answer: report QIAs or S/HSMs to your chain of command or supervision immediately (reference: AFI 14-404, para 2.11.2).

4.1.7. *For* IO purposes, when is imagery considered "collected"?

4.1.7.1. Answer: 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 (reference: DoDM 5240.01, Glossary).

TRACY T. WARD, Colonel, USAF
Deputy Director of Intelligence

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

ACCMAN 14-402, *Unit Level Intelligence Mission & Responsibilities*, 25 March 2020

AFI 10-701, *Operations Security (OPSEC)*, 24 July 2019

AFI 10-801, *Defense Support of Civil Authorities*, 29 January 2020

AFI 14-404, *Intelligence Oversight*, 03 September 2019

AFI 31-101, *Integrated Defense (ID)*, 25 March 2020

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

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

AFMAN 11-502, *Small Unmanned Aircraft Systems*, 29 July 2019

AFMAN 14-405, *Multiple Source, Discipline, and Domain Intelligence, Surveillance, and Reconnaissance (ISR)*, 11 May 2020

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

Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publically Available Information, July 2011

CNGBM 2000.01A, *NG Intelligence Activities*, 11 April 2019

DoD 5240.1-R, *Procedures governing the activities of DoD Intelligence Components that Affect US Persons*, 26 April 2017

DoDD 3025.18, *Defense Support of Civil Authorities (DSCA)*, 29 December 2010

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

DoDD 5148.13, *Intelligence Oversight*, 26 April 2017

DoDD 5240.01, *DoD Intelligence Activities*, 22 March 2019

DoDI 3025.21, *Defense Support of Civil Law Enforcement Agencies*, 8 Feb 2019

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

EO 12333, *US Intelligence Activities*, 4 December 1981

EO 13470, *Further Amendments to EO 12333*, 4 August 2008

Policy Memorandum SecDef, *Domestic use of UAS in US National Airspace*, 18 August 2018

USSID SE3000, *SIGINT Mission of USAF Cryptologic Forces*, 17 Oct 2019

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ACC—Air Combat Command

ACCMAN—Air Combat Command Manual

ACC/A2—Air Combat Command Intelligence Directorate

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigation

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

ANG—Air National Guard

ATKS—Attack Squadron

CAF—Combat Air Forces

CI—Counter Intelligence

COMM—Communications Personnel or Unit

CJCS—Chairman, Joints Chiefs of Staff

CSS—Commander Support Staff

DCGS—Distributed Common Ground System

DIA—Defense Intelligence Agency

DNI—Director, National Intelligence

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DSCA—Defense Support of Civil Authorities

EO—Executive Order

FAQs—Frequently Asked Questions

FI—Foreign Intelligence

FP—Force Protection

FS—Fighter Squadron

G2—US Army Intelligence

GKO—Guard Knowledge Online

GM—Guidance Memorandum

ID—Integrated Defense

IDC—Integrated Defense Council

IG—Inspector General

INTEL—Intelligence

IO—Intelligence Oversight

IOB—Intelligence Oversight Board

IOM—Intelligence Oversight Monitor

IOO—Intelligence Oversight Officer

IP—Internet Protocol

ISP—Internet Service Provider

ISR—Intelligence, Surveillance and Reconnaissance

JA—Judge Advocate

JWICS—Joint Worldwide Intelligence Communication System

MAJCOM—Major Command

MDS—Mission Design Series

MDT—Mission Defense Team

MFR—Memorandum for Record

MICT—Management Internal Control Toolset

NGB—National Guard Bureau

NIPR—Nonsecure Internet Protocol Router

NSA—National Security Agency

NTISR—Non-Traditional Intelligence, Surveillance and Reconnaissance

OG—Operations Group

OPLAN—Operational Plan

OPR—Office of Primary Responsibility

OPSEC—Operations Security

OSINT—Open Source Intelligence

OSS—Operations Support Squadron

PAI—Publically Available Information

POC—Point of Contact

POV—Privately Owned Vehicle

PUM—Proper Use Memorandum

QIA—Questionable Intelligence Activities

RegAF—Regular Air Force

R&D—Research and Development

RPA—Remotely Piloted Aircraft

SAC—Self Assessment Communicator

SF—Security Forces

S/HSM—Significant or Highly Sensitive Matters

SIGINT—Signals Intelligence

SIO—Senior Intelligence Officer

SIOO—Senior Intelligence Oversight Office

SIPRnet—Secure Internet Protocol Router Network

SOP—Standard Operating Procedure

SPP—SharePoint Portal

TDY—Temporary Duty

URL—Uniform Resource Locator

USP—US Person

USPI—US Person Information

USSID—US Signals Intelligence Directive

WG—Wing

WIT—Wing Inspection Team

Attachment 2

LINKS

Table A2.1. Links.

Name	URL
ACC/A2 Unit Support SharePoint Portal (NIPR)	https://cs2.eis.af.mil/sites/12024/a2o/nest/Pages/nest.aspx
ACC/A2 IO SharePoint Portal (NIPR)	https://cs2.eis.af.mil/sites/12024/nest/pages/io.aspx
NGB/J2 IO (requires GKO Access)	https://federation.eams.army.mil/pool/sso/authenticate/l/2?u=https%3A%2F%2Ffederation.ng.mil%2Fadfs%2Fservices%2Ftrust&wa=wsignin1.0&wctx=f0cc3b3d-fd9f-414c-8f98-fc9cdff135db&wtrealm=https%3A%2F%2Ffederation.ng.mil%2Fadfs%2Fservices%2Ftrust - (You'll need to apply for a Guard Knowledge Online (GKO) account to get in - register when you open this link))
DoD Senior IO Official website	https://dodsioo.defense.gov/
AF e-Pubs (access to AF IO pubs)	https://www.e-publishing.af.mil/Product-Index/#/?view=pubs&orgID=10141&catID=1&series=6&modID=449&tabID=131
DoD Issuances (Access to DoD IO pubs)	https://www.esd.whs.mil/dd/
ACC/A2 Policy & Guidance (alt access to AF, ACC and NGB IO pubs)	https://cs2.eis.af.mil/sites/12024/a2o/nest/SiteAssets/Policy.aspx

Attachment 3

INTELLIGENCE OVERSIGHT MONITOR SELF-ASSESSMENT CHECKLIST

A3.1. IO Monitor Self-Assessment Checklist. For use by IO monitor, Senior Intelligence Officer and Superintendent; supplements MICT SAC 14-404.

Table A3.1. IO Monitor Self-Assessment Checklist.

1.	Has the Wing/Group/Squadron commander designated in writing a primary and alternate intelligence oversight monitor? *<u>Note:</u> Ensure Letter of Appointment is in unit continuity book. Also, recommend appointment is by no lower than group commander.*	AFI 14-404, para 2.9.2
2.	(On behalf of the Commander/Director) Ensure IO training is conducted, as required, to include annual refresher training and initial IO training 60 days after assignment. *<u>Note:</u> Can include Judge Advocate and Wing IG. Ensure initial and recurring training is documented in personnel training records and IOM training tracker. Incorporate annual IO training into internal and external training plans as required.*	AFI 14-404, para 2.9.6 and 2.10.2
3.	a. Does the IO training incorporate or is it based on the ACC/A2 baseline IO training (i.e., the most current information)? *<u>Note:</u> Use the ACC/A2 baseline training to develop local IO training in order to be sure information is current. Found at:* https://cs2.eis.af.mil/sites/12024/a2o/nest/SiteAssets/Policy.aspx?PageView=Shared&InitialTabId=Ribbon.WebPartPage&VisibilityContext=WSSWebPartPage	
4.	Does the unit retain a hard or electronic copy of all required reference materials? Are the references in training materials and IO cards current and valid? *<u>Note:</u> Maintain hardcopy, electronic copies and/or links to all required references:* *a. DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, Interim Change 2, dated 26 Apr 17* *b. DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities, dated 08 Aug 16* *c. DoDD 5240.01, DoD Intelligence Activities, Interim Change 2, dated 29 Aug 17* *d. DoDD 5148.13, Intelligence Oversight, dated 26 Apr 17* *e. Air Force Instruction (AFI) 14-404, Intelligence Oversight, dated 03 Sep 19*	AFI 14-404, para 2.10.1

	Current reference materials found at: https://cs2.eis.af.mil/sites/12024/nest/pages/io.aspx	
5.	Are unit members and staff personnel aware of the applicability of IO to them and the unit's mission? *<u>Note:</u> Ensure proper use of cited information is covered in initial and annual refresher training. Local IO wallet card - all personnel requiring IO should carry, can spell out IO applicability to the unit's mission.*	AFI 14-404, para 2.10.1
6.	Are unit members and staff personnel aware there are specific procedures and restrictions on providing intelligence support to law enforcement agencies?	DoD 5240.1-R, Chapter 12, C12.2.1 through C12.2.2.5
7.	Are unit members and staff personnel aware of what questionable intelligence activities are and mandated reporting procedures?	AFI 14-404, para 2.11.2
8.	Do unit members and staff personnel understand "US persons" pertains to associations, corporations, and resident aliens as well as US citizens?	DoD 5240.1-R, DL1.1.25 - DL1.1.25.3 (begins on page 12)
9.	Are unit personnel aware of the procedures to collect, retain, or disseminate publically available information?	AFI 14-404 para 4.3 thru 4.3.2; DoDM 5240.01, 3.2 Procedure 2
10.	Has the IOM developed program management materials (e.g., procedures, instructions, checklists, continuity book), and a training tracker? Is the training tracker up to date? Are there procedures in place to ensure everyone receives their initial and annual refresher training when required? Are procedures in place to ensure unit members required IO training who are deploying or going on extended TDYs do not lapse in IO training while departed?	ACCI 14-202, para 2.1.1.

Attachment 4

EXAMPLES

A4.1. Intelligence Oversight Continuity Binder Contents

A4.1.1. The IO Monitor should maintain the unit IO Continuity Binder.

A4.1.2. The binder may be in electronic or hardcopy format and should contain the following, at a minimum. Unless otherwise indicated, records will be maintained for the period indicated in records management guidelines IAW reference pp.

A4.1.2.1. Appointment letters for primary and alternate IO Monitors.

A4.1.2.2. IO Monitor duties and responsibilities.

A4.1.2.3. Unit-tailored IO training.

A4.1.2.4. IO training records (initial, annual, and pre-deployment) -- maintain for three years. Use Service-specific systems of record for maintaining IO training records but also ensure that IO monitors can access and validate completeness of training records.

A4.1.2.5. Copies of Executive Order 12333, DoD Directive 5240.01,DoD Manual 5240.1-R, DoD Directive 5148.13, AFI 14-404.

A4.1.2.6. Copy of MICT SAC for AFI 14-404.

A4.1.2.7. Self-inspection and inspection records -- maintain for three years.

A4.1.2.8. QIA, S/HSM and Federal crime reporting process and report format.

A4.1.2.9. Copies of any QIA, S/HSM, and Federal crime reports -- maintain for three years.

A4.1.2.10. Annual file review certification MFR -- maintain for three years.

Figure A4.1. Quarterly Intelligence Oversight Report Template.

[DoD Component] 1st QUARTER CYXX INTELLIGENCE OVERSIGHT REPORT

1. New Incidents

a. File Number (e.g.., DIA 2017-01-Q)

(1) Incident Description:

(2) Timeline: (Indicate when the incident occurred, when it was initially reported within the DoD Component, and when it was reported to the DoD SIOO; if applicable, explain any delay in reporting.)

(3) Reason for Report: (For a QIA, identify the specific law or policy violated. For an S/HSM, identify the rationale for reporting as such.)

(4) Cause: (Indicate how or why the incident occurred.)

(5) Impact on National Security or International Relations:

(6) Impact on Civil Liberties or Privacy:

(7) Remedial Action:

(8) Additional Information: (Provide any additional information required to fully inform the Secretary of Defense, the Deputy Secretary of Defense, the IOB, and the DNI, or provide context about the incident.)

(9) Status: (Indicate whether the incident is open or closed. If open, provide the status of the ongoing investigation. If closed, include a notation indicating whether any allegations were substantiated or not substantiated.)

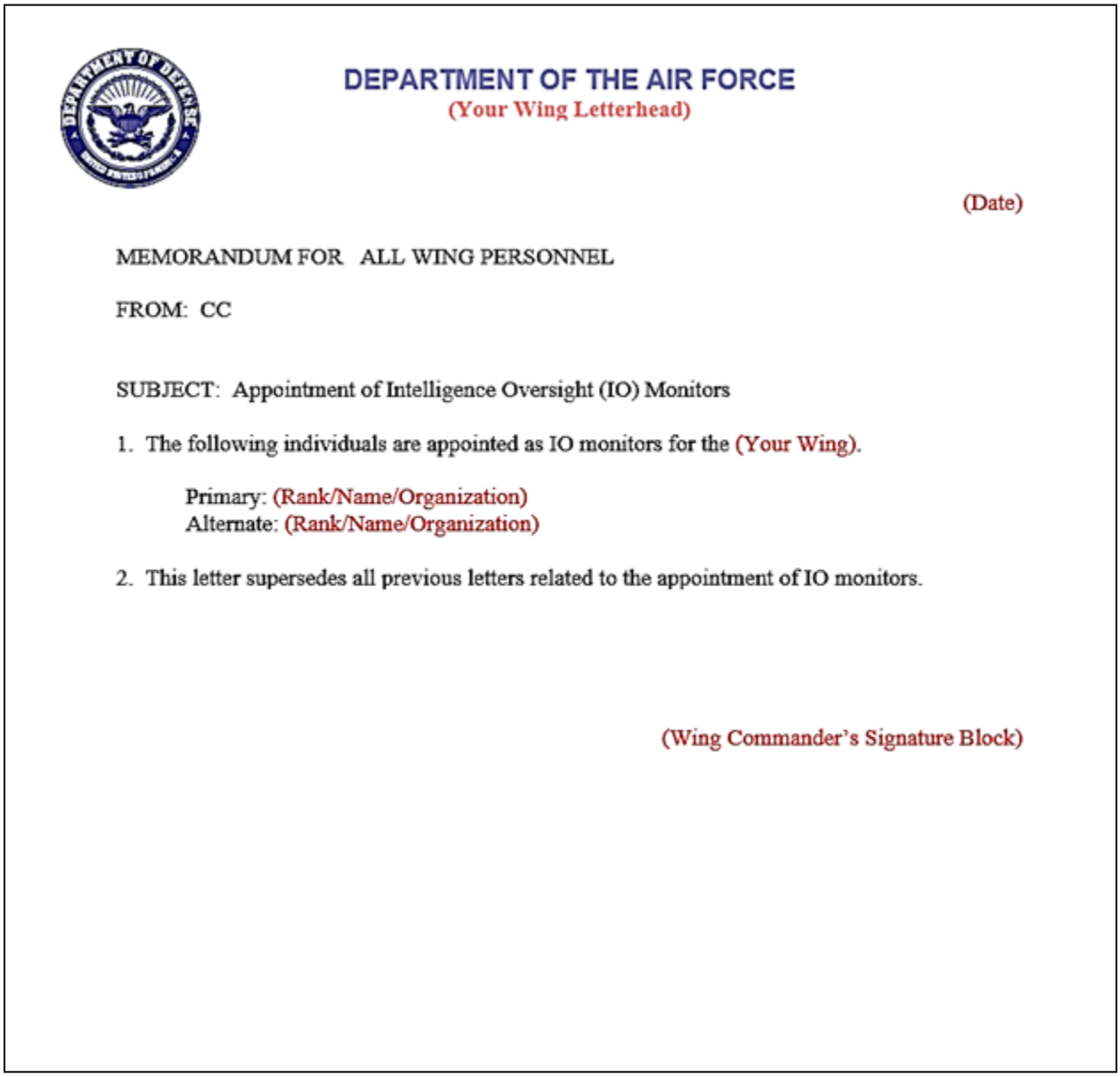
2. Previously Reported Incidents: (Use the same format as Section 1 for previously reported incidents still under investigation as well as those resolved and closed during the quarter.)

3. Crimes Reported: (Provide a narrative summary of any intelligence or intelligence-related activity that has been or will be reported to the US Attorney General, or that must be reported to the US Attorney General as required by law or other directive, including crimes required by E.O. 12333 to be reported to the US Attorney General.)

4. Trend Analysis: (Include metrics and identify and explain common causal factors; include data over a timeframe appropriate for the type of activities reported.)

5. Significant Inspection Findings/Intelligence Oversight Program Developments: (Provide a description of any significant internal inspection findings or intelligence oversight program developments.)

Figure A4.2. IO Appointment Letter Template.



DEPARTMENT OF THE AIR FORCE
(Your Wing Letterhead)

(Date)

MEMORANDUM FOR ALL WING PERSONNEL

FROM: CC

SUBJECT: Appointment of Intelligence Oversight (IO) Monitors

1. The following individuals are appointed as IO monitors for the (Your Wing).

   Primary: (Rank/Name/Organization)
   Alternate: (Rank/Name/Organization)

2. This letter supersedes all previous letters related to the appointment of IO monitors.

(Wing Commander's Signature Block)

Figure A4.3. IO Tri-Fold Brochure Example, Page 1.

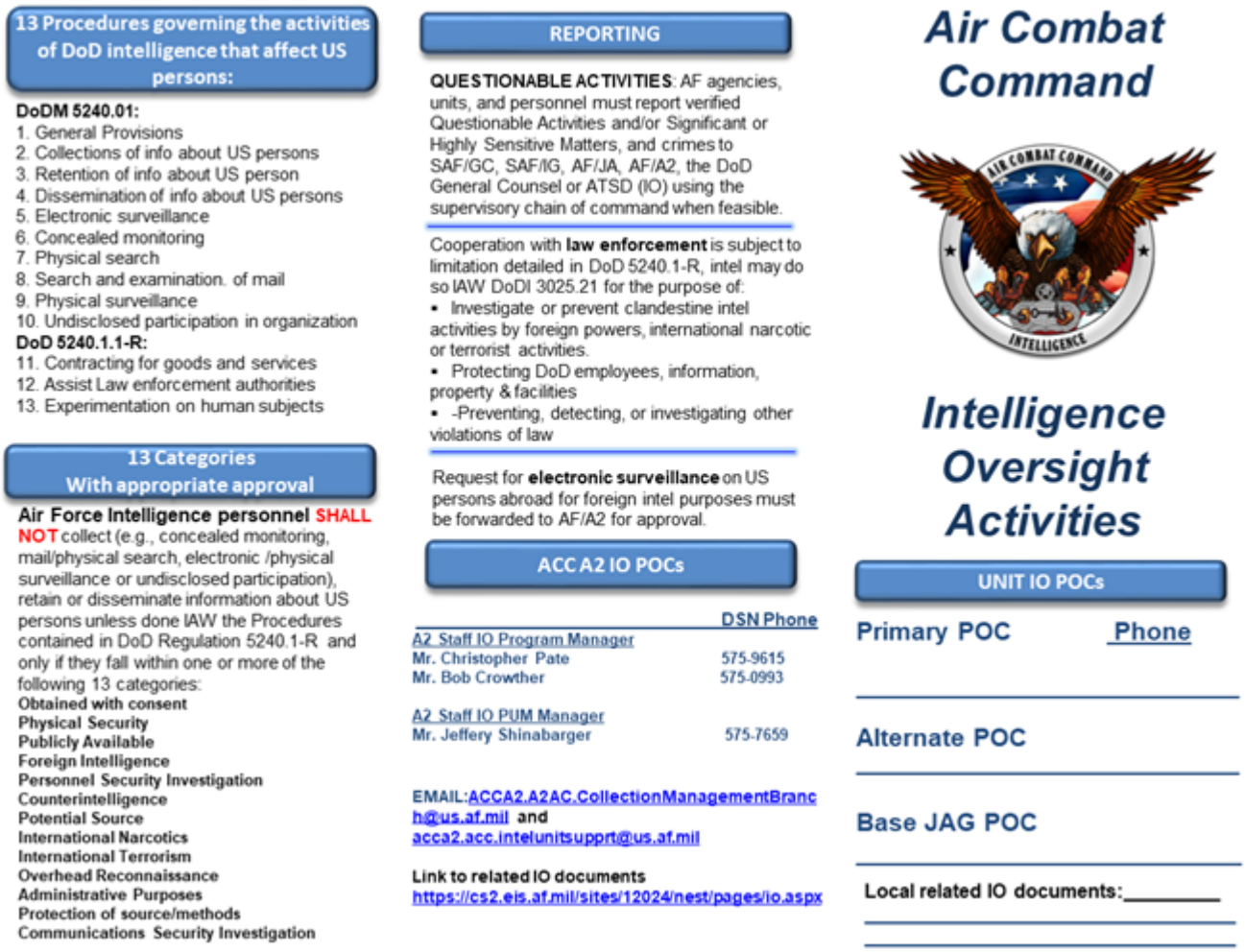


Figure A4.4. IO Tri-Fold Brochure Example, Page 2.

Readiness

PURPOSE

IO involves a balancing of two fundamental interests:

1. Obtaining the intel info required to protect national security
2. While protecting individual rights guaranteed by the Constitution and outlined with the laws of the United States.

Primary objectives is to Mitigate infringement upon the rights of US persons by ensuring intel personnel at all levels understand IO responsibilities

SCOPE

Applies to **all** military intel units, staff orgs, civilian-contracted orgs and non-intel orgs that perform intel-related activities that could collect, analyze, process, retain, or disseminate info on US persons.

U.S. Person

U.S. Person is a U.S. Citizen: a known permanent resident alien; or, a corporation (if incorporated in the U.S., and not directed and controlled by a foreign government). Any person or organization located outside of the U.S. is presumed not to be a U.S. person UNLESS there is specific information to the contrary.

INDIVIDUAL RESPONSIBILITIES

Complete : initial IO training after assignment/employment; and complete annual refresher training; as well as any unit specific training.

Products

COLLECTION

Information is considered "**collected**" only when it is has been received for use by an employee of a DoD intelligence component in the course of official duties.

Data acquired by electronic means is "collected" only after it has been processed into intelligible form.

IMAGERY

DOMESTIC: is any imagery collected by satellite (national or commercial) and airborne platforms that cover the area of the 50 US States, District of Columbia, territories & possessions, 12nm seaward limit of these land areas.
-Use only when there is a justifiable need to do so

Legal valid requirements

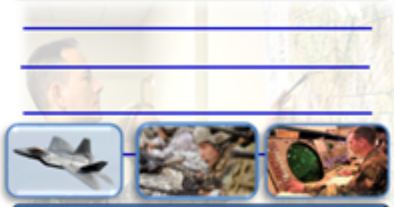
- Natural Disaster
- Counterintelligence, FP, & Security-related Vulnerability Assessments
- Environmental Studies
- Exercises, Training, Testing, or Navigational Purposes

Satellites: NGA has legal review & approval for the collection and dissemination of imagery from national satellites.

AF Platforms: Approved PUM on file before airborne, tactical DoD satellite platforms, or ground platforms can be tasked to collect domestic imagery
- Tactical Satellites are considered "airborne" platforms and so PUM approval authority dose not reside with NGA its MAJCOM level.

Organization

Know Unit mission as it relates to IO



Policy & Guidance Documents

NSGM FA 1806.5: Domestic Imagery.
NSGM CS 9400.04: Commercial Remote Sensing Satellite Imagery Policy.

EO 12333: Established the Oversight Program, clarified authority and responsibilities of US intelligences agencies and serves as the basis for other oversight directives

DoDM 5240.01, DoD 5240.1-R, & DoDD 5148.13: Provide the authorities by which DoD intelligence components may collect, retain and disseminate information concerning U.S. person; also contains the reporting structure for possible violations.

AFI 14-404, dated 04 Sep 19: Implements EO 12333 and DoD 5240.1-R. Document gives directive to USAF intelligence activities. To ensure units and staff organization conducting Intel ops do not infringe on or violate the rights of a US person

USSID SP0018: Classified document which defines policies and procedures and assigns responsibilities to ensure the missions and functions to the U.S. SIGINT system are conducted in a manner that safeguards the Constitutional right of U.S. Persons

Figure A4.5. IO Wallet Card Example, Side 1.

INTELLIGENCE OVERSIGHT

Unit IO Monitors:
PURPOSE: Protect national security without violating Constitutional rights of US persons. **RESPONSIBILITIES:** All intelligence personnel must abide by rules and regulations contained within stated IO guidance and report infractions to their chain of command or IO monitor. **SCOPE:** Applies to **all** personnel assigned to an Intelligence unit regardless of AFSC or location. **US PERSON:** US Citizen/known permanent resident alien/US corporation (if incorporated in US & not directed/controlled by a foreign gov't) Any person or organization located outside the US is presumed *not* to be a "US person" UNLESS there is specific information to the contrary. **DOMESTIC IMAGERY:** includes 50 States, DC, territories & possessions, 12nm seaward limit. **REFERENCES: NSGI 1806:** Domestic Imagery**. EO 12333:** Established Oversight Program, clarified authority, responsibilities of US intelligences agencies and basis for other directives. **DoDM 5240.01:** Provides sole *authority* DoD intelligence components may collect, retain, and disseminate information concerning US persons; also contains reporting structure for possible violations. **DoDD 5148.13:** Establishes policies, assigns responsibilities, provides procedures for employee conduct and identifying/reporting questionable Intel activities (QIAs) and significant /highly sensitive matters. **AFI 14-404:** Implements Air Force Policy Directive 14-4, *Management of the Air Force Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise*. Directive to USAF intelligence actions and with DoDM 5240.01, is the IO authority for USAF. **USSID SP0018**: Classified document that defines policies /procedures, assigns responsibilities to ensure mission/functions of SIGINT are conducted in manner that safeguards US Persons' Constitutional rights.

Figure A4.6. IO Wallet Card Example, Side 2.

REPORTING QUESTIONABLE INTEL ACTIVITIES: Any intelligence activity that may violate law/Executive Order/Presidential Directive/applicable DoD policy must be reported IAW DODD 5148.13. **REPORT TO CHAIN OF COMMAND Lawful collections against US Persons**: Three step process: **Right Mission**--Must be part of your unit's mission; **Right Procedures**-- Collection must fit into one of **DoD 5240.1-M c**ategories; **Approval --** Collection must be approved by **AF/A2** (AFI 14-404 Attachment 2, Fig. 2.1.) **"Collected" - Information** is collected when it is received by a Defense Intelligence Component, whether or not it is retained for intelligence or other purposes. **USAF Intelligence personnel SHALL NOT** collect (e.g., concealed monitoring, mail/physical search, electronic /physical surveillance or undisclosed participation), retain or disseminate information about US persons unless done IAW the Procedures contained in **DoD Regulation 5240.1-M. Questionable Intel Activity** - any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, or applicable DoD policy. **Sensitive/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 E.O., 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. **Reporting**: Report any QIA/S/HSM immediately to your IO monitor or Chain of command. See DoDD 5148.13 for additional information. Link To related IO Documents: https://cs2.eis.af.mil/sites/12024/nest/pages/io.aspx

Figure A4.7. Unit IO Standard Operating Procedures Example.

XX OPERATIONS GROUP (ACC)

XX STANDARD OPERATING PROCEDURES 14-X

JOINT BASE XXXXXXXXXXX
1 Mar 2020

Intelligence

INTELLIGENCE OVERSIGHT PROGRAM

OPR: XX OG/CC Certified by: XX OSS/IN (Col XXX X. XXXX)

Pages: 3

Supersedes: XX OG OI 14-6, 1 March 2018 Distribution:XX OSS, XX FS, XX FS

This Standard Operating Procedure (SOP) delineates responsibilities and procedures for the XX Operations Group (OG) Intelligence Oversight (IO) Program. This OI applies to all assigned intelligence sections and personnel. This SOP ensures the information required to protect national security is obtained while simultaneously protecting individual rights guaranteed by the Constitution and laws of the United States.

REFERENCES:

ACCMAN 14-402, *Unit Level Intelligence Mission & Responsibilities*, 25 March 2020

AFI 14-1020, *Intelligence Mission Qualification and Readiness*, 8 November 2017

AFI 14-404, *Intelligence Oversight*, 3 September 2019

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

DoD 5240.1-R, *Procedures governing the activities of DoD Intelligence Components that Affect US Persons*, 26 April 2017

DoDD 3025.18, *Defense Support of Civil Authorities (DSCA)*, 8 Feb 2019

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

DoDD 5148.13, *Intelligence Oversight*, 26 April 2017

DoDD 5240.01, *DoD Intelligence Activities*, 22 March 2019

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

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

Executive Order 12333, US Intelligence Activities, 4 December 1981

Executive Order 13470, Further amendments to EO 12333, 4 August 2008

SECDEF Policy Memorandum, *Domestic use of UAS in US National Airspace*, 18 August 2018

1. RESPONSIBILITIES:

1.1. The Commander will:

1.1.1. Oversee the XX WG IO program and appoint in writing IO program monitors (primary and alternate) as required by AFI 14- 404, para 2.9.2.

1.1.2. Ensure compliance with all intelligence oversight rules when conducting intelligence or intelligence-related activities as required by AFI 14-404, para 2.9.1.

1.1.3. Ensure IO violations are reported in accordance with governing directives as required by DoDM 5148.13, Section 4 and AFI 14- 404, para 2.9.3.

1.1.4. Investigate Questionable Intelligence Activities and/or Significant/Highly Sensitive Matters using procedures for commander-directed investigations IAW AFI 90-301, *Inspector General Complaints Resolutions.*

1.1.5. Administer an intelligence oversight training program which provides all employees who conduct intelligence or intelligence related activities with initial, pre-deployment and annual refresher content tailored to mission requirements as required by AFI 14-404, para 2.9.6.

1.2. The Intelligence Oversight Program Monitor will:

1.2.1. Manage and implement the IO program. Make available applicable executive orders, directives, regulations and instructions relative to IO and maintain the IO program continuity binder.

1.2.2. Administer an IO training program that is tailored to mission requirements and provides initial, pre-deployment and annual refresher IO training to all applicable employees.

1.2.2.1. Ensure all newly assigned intelligence personnel complete the ACC Baseline IO Training Program hosted on the ACC/A2 Unit Readiness SPP, Intelligence Oversight section: https://cs2.eis.af.mil/sites/12024/nest/pages/io.aspx. IO Training will be completed within 60 days upon arriving at duty location. This initial training will be documented on the individual's Initial Qualification Training (IQT) checklist.

1.2.2.2. Monitor initial and annual IO training for all senior leadership who command Intelligence or Information Operations units (to include Operations Group Intelligence). At a minimum, monitor training for: WG/CC, WG/CV, OG/CC, OG/CD, OSS/CC, OSS/DO, and FS/CCs. Engage with the ABW/JAG and WG/IG members responsible for units that perform intelligence activities, as defined in AFI 14-404, paragraphs 4.9 and 4.10, for prompt completion of IO training.

1.2.3. Ensure all X OSS, XX FS, and XX FS intelligence personnel complete the ACC/A2 IO Baseline Training initially and at least annually and within 30 days prior to deployment.

1.2.4. Provide assistance in rendering collectability determinations on information acquired about US persons within 90 days as outlined in AFI 14-104, paragraph 11.2. Report any questionable activity that constitutes or is related to intelligence activity that may violate law, policy, intelligence oversight directives or regulations.

1.2.5. Develop and execute additional training as required, IO evaluation tools and self-assessment programs. Additionally, serve as a Wing Exercise Evaluation Team member for these programs only.

1.2.6. Periodically review the units' produced intelligence products and related activities for compliance with applicable standards.

1.2.7. Assist the commander in the administration of IO by monitoring the accomplishments of the units' responsibilities IAW DoDD 5148.13.

1.3. Airmen, government civilians, and contractors who conduct intelligence and intelligence-related activities for the USAF will:

1.3.1. Understand the role of IO within the organization.

1.3.2. Complete initial IO training within 60 days of assignment, annual refresher training and pre-deployment training as necessary.

1.3.3. Be familiar with AFI 14-404 and any organization-specific instructions concerning IO.

1.3.4. Conduct all assigned intelligence and/or intelligence related activities IAW all applicable laws and policies.

1.3.5. Report Questionable Intelligence Activities or Significant/Highly Sensitive Matters to their chain of command or supervision immediately.

XXXXXXX X. XXXXX, COL, USAF

Commander