Adjutant General's Department
Headquarters, Kansas National Guard
5920 SE Coyote Drive
Topeka, Kansas 66619
08 December 2016

KSNG SOP 381-10

Kansas National Guard Intelligence Oversight Standard Operating Procedures

By order of the Adjutant General:

ROGER D. MURDOCK
COL, KSNG
Chief of Staff, Joint Forces Headquarters

Official:

CHRISTOPHER A. STRATMANN
Col, KSNG
J2/6, Director of Intelligence & Communications

History. This issue publishes a revision of this publication.

Summary. This publication establishes policies and procedures governing the KSNG Military Intelligence Oversight program.

Supplementation. Supplementation of this publication is prohibited.

Suggested Improvements. The proponent of this publication is the JFHQ-KS-J2. Users are invited to send comments and suggested improvement to The Adjutant General's Department, ATTN: JFHQ-KS-J2, 2722 SW Topeka Blvd, Topeka, KS 66611-1287

Distribution. A

This SOP supersedes KSARNG SOP 381-10, dated 15 December 2013

Contents

Contents – Continued

Chapter 1 - General

1-1. Applicability
Applicable to all members of the Kansas National Guard (KSNG) assigned or attached to intelligence units or staffs, all members with an intelligence Military Occupational Specialty (MOS) or Air Force Specialty Code (AFSC), the Kansas Analysis Center (KAC), and all other areas involving intelligence or intelligence related activities and non-intelligence organizations that perform intelligence or intelligence-related activities.

1-2. Purpose
a. Establish standard operating procedures concerning the collection, analysis, maintenance, and dissemination of intelligence information by KSNG personnel.
b. Identify intelligence oversight training requirements.
c. Establish procedures for reporting questionable and/or potentially questionable activities or procedures IAW NGR 20-10, AR 381-10, AFI 14-104.
d. Ensure that units and staff organizations conducting intelligence activities do not infringe on or violate the rights of US persons.

1-3. Definition
Intelligence Oversight (IO) is the process of ensuring that all Department of Defense (DoD) intelligence, counterintelligence, and intelligence related activities are conducted in accordance with applicable U.S. law, Presidential Executive Orders, and DoD directives and regulations. The DoD Intelligence Oversight program has two main objectives. First and foremost is prevention of violations. Through training and awareness programs, the DoD hopes to increase understanding of the activities that our intelligence organizations and personnel may, and may not, perform to accomplish their mission lawfully and in accordance with DoD policy. The program is designed to ensure that the DoD can conduct its intelligence and counterintelligence missions while protecting the statutory and constitutional rights of U.S. persons. Second, when prevention fails, the DoD needs to identify, investigate, and report violations, and implement corrective actions to ensure there are no recurrences.

1-4. Policy
a. Army National Guard (ARNG) and Air National Guard (ANG) members serving in a Title 10 (T-10) status must comply with Service-specific guidance IAW AR 381-10 and AFI 14-104.
b. NG intelligence personnel operating in a Title 32 (T-32) status operate as members of the DoD intelligence component and must comply with all DoD guidance and Federal laws applicable to the component.
c. Federal intelligence and Intelligence, Surveillance and Reconnaissance (ISR) equipment is not used for activities other than for Foreign Intelligence (FI) or Counterintelligence (CI) unless approved by the Secretary of Defense (SecDef) or his or her designee IAW DoD 5240.01-R, Change 1, 8 Aug 2016.
d. NG intelligence personnel operating in a State Active Duty (SAD) status are not members of the DoD intelligence component and are prohibited from engaging in DoD intelligence and CI activities, and from using DoD intelligence and CI equipment, such as the Joint Worldwide Intelligence Communications System, unless the SecDef or his or her designee authorizes that use IAW DoD 5240.01-R, Change 1, 8 Aug 2016.

1-5. References
Required publications are listed in Appendix A.

Chapter 2 - Intelligence Oversight Program

2-1. Intelligence Oversight Monitor

a. The primary and alternate IO Monitors for the Kansas National Guard are recommended by the J2 Senior Intelligence Officer (SIO) and appointed by the Adjutant General.
b. State IO Monitor, as assigned by the J2 SIO, will request from G1/A1 monthly updates of personnel who are newly assigned to an intelligence section and/or who receive an intelligence MOS/ AFSC.
c. Each major subordinate command, battalion/squadron and higher and/or any units/activities involved in intelligence activities will appoint a Primary and an Alternate IO Monitor. IO Monitors will be appointed by memorandum (see Appendix B) signed by the unit/activity commander. A copy of the appointment will be provided to the State IO Monitor ATTN: J-2 Intelligence Oversight Monitor.
d. IO Monitors will ensure IO training is conducted IAW the standards listed in Appendix A.
e. Each IO Monitor will maintain a copy of training and inspection documentation in addition to this publication and each of the required references listed in Appendix A in a tabbed notebook referred to here after as the "IO Continuity Binder" (see Appendix C) and/or in soft copy saved electronically.
f. Each Intelligence Unit and/or IO Monitor will maintain a current, full roster of personnel assigned to the unit's intelligence section and a list of commanders (and date assigned) in the IO Continuity Binder so the IO monitors can easily track who requires IO training (Initial and Annual Refresher) and when they require IO training.
g. IO Monitors will inspect intelligence functions and activities of subordinate units IAW the checklist in Appendix D.

2-2. Intelligence Oversight Training

a. Upon assignment to an intelligence section, Kansas Joint Forces Headquarters Sensitive Compartmented Information Facility (SCIF), or other intelligence activities and duties, Soldiers and Airmen will receive initial IO training from the unit IO Monitor no later than 90 days after assignment. As a minimum, this training will include applicable regulations/SOPs, restraints, guidelines of the duty, minimum familiarity standards (Procedures 1-4, 12, 14, 15), and training tailored towards the intelligence mission you are assigned to. This briefing will be documented using the IO Training Register (Appendix E).
b. All personnel assigned to intelligence sections or other intelligence activities will receive annual refresher training. This training will be provided by the unit IO Monitor and include applicable regulations/SOPs, restraints, guidelines of duty, and minimum familiarity standards (Procedures 1-4, 12, 14, 15). This training will be documented using the IO Training Register.
c. Units will include IO training on their unit Yearly Training Plan and unit training schedules.
d. Units will ensure that unit Commanders and the A-3/S-3 are included in Initial and Refresher IO training.
e. KSARNG Units will document IO training through the Digital Training Management System (DTMS).
f. KSANG Units will document IO training through the Advanced Distributed Learning System (ADLS).
g. Units are required to retain IO training documentation for a minimum of 5 years.
h. NGB provided Intelligence Oversight training is available through the KSNG-IG website or from the State IO monitor.
i. Units will document annual intelligence file reviews through a Memorandum for Record (MFR) (Appendix F).

2-3. Compliance Inspections

a. Compliance inspections will be conducted as part of each command unit's Organizational Inspection Program (OIP) (Appendix J).
b. Inspector General (IG) inspectors will inspect unit IO Continuity Binders and electronic copy folders as well as question applicable personnel to assess their knowledge of IO.
c. IO Continuity Binders and/or electronic copy folders will comply with Appendix C.

2-4. Specific Limitations

a. National Guard personnel, facilities and/or equipment assets WILL NOT BE USED to collect, analyze, retain, or disseminate information concerning U.S. persons except as lawfully directed in references listed in Appendix A.
b. The unit must first have the mission and authority to conduct the intelligence activities.
c. Intelligence support to force protection may only involve identifying, collecting, reporting, analyzing and disseminating intelligence regarding foreign threats unless the SecDef or his or her designee authorizes additional support IAW DoD 5240.01-R, Change 1, 8 Aug 2016.
d. Civilian Federal, State, and local law enforcement authorities have the primary responsibility for information collection to protect U.S. military forces within the United States. However, information received by intelligence activities identifying U.S. persons who are alleged to threaten the force must be passed to the threatened commander and the organization responsible for countering that threat (e.g., State Anti-terrorism Program Coordinator, applicable Law Enforcement Agencies). The responsibility of force protection resides with J3 DOMS.

2-5. Intelligence Operations

a. The following guidance applies to Counterintelligence (CI) activities:
    1) Counterintelligence involves gathering information and performing activities to protect against espionage, other intelligence activities, international terrorist activities, sabotage, or assassinations conducted for or on the behalf of foreign powers, organizations, or persons.
    2) KSNG personnel could become involved in a counterintelligence mission upon mobilization or by functioning in direct support of an active component organization IAW AR 381-20.
    3) There are no National Guard units authorized to engage in counterintelligence activities, excluding training.
    4) National Guard members cannot conduct domestic counterintelligence activities in a Title 32 duty status.
    5) Other possible CI activity falls under the jurisdiction of the Federal Bureau of Investigation (FBI). This delineation of responsibility is based on "The Agreement between the Deputy Secretary of Defense and Attorney General, April 05, 1979", an extract of which is annotated on page 17 of AR 381-10. This reference clearly indicates that the National Guard does not have the independent authority necessary to engage in counterintelligence missions, except for training purposes only.
b. Imagery Intelligence (IMINT) can include photographic, infrared, radar, and electro-optic tools and systems that capture images using ground or areal based systems. These systems, once confined to terrain mapping or for use in military exercises are now used in support of counter-drug operations. As long as these systems are not targeted against U.S. Persons, and Guard members are following the guidelines of NGR (AR) 500-2 and NGR (AF) 55-6, training exercises can employ this equipment.
c. Unmanned Aircraft Systems (UAS). Unless permitted by law and approved by the SecDef, NG personnel using DoD funded UAS for domestic operations may not conduct surveillance on U.S. persons. UAS may not be used for Federal, State, or local immediate response. All units that have UAS, remotely piloted aircraft (RPA) or commercial off-the-shelf (COTS) UAS, such as Quad copters, must have a copy of CNGBI 7500.00 in their IO Continuity Binders and are required to have an approved Proper Use Memorandum (PUM) for all UAS missions and SecDef approval for all UAS used for non-DoD-required training.
d. PUM. Requests for a PUM should be submitted through the State IO monitor at 785-646-1706.

2-6. Procedures

Each National Guard member assigned to an S-2/G-2 section or other intelligence activity will, as a minimum, be familiar with Procedures 1-4, 12, 14 and 15.

A U.S. citizen is defined as:

a. A U.S. citizen by birth or naturalization.
b. An alien known by the Defense Intelligence Component concerned to be a permanent resident alien.

c. An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
d. 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.
e. 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.

USPI does not include:

a. A reference to a product by brand or manufacturer's name or the use of a name in a descriptive sense, as, for example, Ford Mustang or Boeing 737; or
b. Imagery from overhead reconnaissance or information about conveyances (e.g., vehicles, aircraft, or vessels) without linkage to additional identifying information that ties the information to a specific U.S. person.

a. PROCEDURE 1: General Provisions. If collecting information on U.S. persons, remember that:

1) Conduct all intelligence activity IAW the U.S. Constitution, laws, Executive Orders, Presidential directives and applicable policy.
2) Mission and Authority must be specified.
3) The activity must not infringe upon a U.S. persons constitutional rights and/or right to privacy.
4) The intrusion must be limited to the least intrusive type possible.
5) The National Guard is not authorized to conduct independent intelligence activities.
6) Do not participate in or request any person or entity to undertake any activities that are forbidden by E.O. 12333 or DoDM 5240.01.
7) Do not engage in any intelligence activity, including dissemination to the White House, for the purpose of affecting the U.S. political process.
8) Collect no more information than is reasonably necessary.

b. PROCEDURE 2: Intentional Collection of USPI. USPI may intentionally be collected only if the information sought is reasonably believed to be necessary for the performance of an authorized intelligence mission or function assigned to the unit/activity, and if the USPI falls within one of the following categories:

1) Publicly available information.
2) Consent is given.
3) Foreign Intelligence (FI). The information is reasonably believed to constitute FI and meets the definitions listed in DoDM 5240.01 Paragraph 3.2 c. (3).
4) Counterintelligence. The information is reasonably believed to constitute CI and meets the definitions listed in DoDM 5240.01 Paragraph 3.2 c. (4).

5) Threats to Safety. Only if the information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations and the threat has a foreign connection.
6) Protection of intelligence sources, methods and activities.
7) Current, former or potential sources of assistance to intelligence activities.
8) Persons in contact with sources or potential sources.
9) Personnel security investigation.
10) Physical security of DoD personnel, installations, operations or visitors.
11) Communications security investigation.
12) Overhead and airborne reconnaissance.
13) Information required for administrative purposes.

Information is considered collected upon receipt. If USPI is intentionally collected, the unit/activity will evaluate the information promptly. If necessary, the unit/activity may retain the information for evaluation for up to 5 years.

c. PROCEDURE 3: Retention of USPI. Information regarding USPI may be kept in National Guard facilities only if it meets the following criteria:

Permanent Retention:
1) The individual concerned has given consent, or
2) Reasonable belief that retention of the USPI is necessary to perform an intelligence mission or function
3) Information was lawfully collected or disseminated, AND
4) One of the following:
    i. Information falls within an approved category of information (PROCEDURE 2), or
    ii. Information is necessary to understand or assess FI or CI

Evaluation Period (Temporary Retention):
1) 5 or 25 years based on the location of the intended target of collection and type of collection.

Information must have controlled access and limited to need-to-know. Identify and mark/tag files believed or known to contain USPI whether electronic or hard copy. Review files periodically to ensure policy and retention periods are being met; maintain letter of certification. PROCEDURE 3 does NOT apply when information is retained for administrative purposes or is required by law to be maintained.

Delete all USPI when:
1) Permanent retention standard has not been met, OR
2) A determination concerning retention standard cannot be met within specified evaluation period.

d. PROCEDURE 4: Dissemination of USPI. Information collected by the National Guard may be disseminated to the following:

1) Any person or entity only if the information is publicly available or the information concerns a U.S. person who has consented to the dissemination.
2) Other Intelligence Community elements. For the purpose of allowing the recipient to determine whether the information is relevant to its responsibilities and can be retained.
3) Other DOD elements to include contractors if recipient is reasonably believed to have a need for such information for the performance of its lawful missions or functions.
4) Other Federal government entities if recipient is reasonably believed to have a need for such information for the performance of its lawful missions or functions.

5) State, Local, Tribal or Territorial governments if recipient is reasonably believed to have a need for such information for the performance of its lawful missions or functions.
6) Foreign governments or International Organizations. KSNG intelligence units or activities will not disseminate USPI to Foreign governments or International Organizations without prior approval from NGKS-J2.
7) Assistance to the Component. Dissemination is to a governmental entity, an international entity, or an individual or entity not part of a government and is necessary for the limited purpose of assisting the Component in carrying out an authorized mission or function. Refer to DoDM 5240.01 for restrictions.
8) Protective Purposes. Dissemination is to a governmental entity, an international organization, or an individual or entity not part of a government, and is necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security.
9) Required Disseminations. Dissemination is required by statute, treaty, Executive order, Presidential directive, National Security Council guidance, policy, memorandum of understanding, or agreement approved by the Attorney General, or court order.

Any dissemination that is not for foreign intelligence, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes, the NGKS-J2 or delegee must approve the dissemination.

e. PROCEDURE 5: Electronic Surveillance.
1) All electronic surveillance must comply with the Fourth Amendment to the Constitution.
2) Only the Attorney General or a judge of the Foreign Intelligence Surveillance Court (FISC) may authorize electronic surveillance, as that term is defined in Foreign Intelligence Surveillance Act of 1978 (FISA), for intelligence purposes in the United States, except for emergency situations in accordance with DoDM 5240.01 Paragraph 3.5.g.
3) Authority to approve the submission of applications or requests for electronic surveillance under FISA or Section 2.5 of E.O. 12333 is limited to the SecDef, the Deputy SecDef, the Under Secretary of Defense for Intelligence (USD(I)), the Secretary or Under Secretary of a Military Department, or the Director of the National Security Agency (DIRNSA/CHCSS).

f. PROCEDURE 6: Concealed Monitoring.
This procedure governs concealed monitoring of any person inside the United States or any U.S. person outside the United States for an authorized FI or CI purpose by a Defense Intelligence Component or anyone acting on their behalf.

No intelligence unit or activity in the KSNG has the authority to conduct concealed monitoring without prior approval from the NGKS-J2 and NGKS-JAG. Any activity under PROCEDURE 8 without the required mission or authority constitutes a Questionable Intelligence Activity (QIA) and must be reported immediately (Appendix G).

g. PROCEDURE 7: Physical Searches.
1) This procedure applies to nonconsensual physical searches for intelligence purposes of any person or property in the United States and of U.S. persons or their property outside the United States that are conducted by Defense Intelligence Components or anyone acting on their behalf.
2) Only CI elements of the Military Services with CI investigative authority may be authorized to conduct physical searches directed against active-duty military personnel for intelligence purposes.
3) Except for searches directed against active-duty military personnel authorized in accordance with DoDM 5240.01 Paragraph 3.7.c., a Defense Intelligence Component may not conduct a physical search of any person or property in the United States for intelligence purposes. This includes both U.S. and non-U.S. persons. A Component may request the FBI to conduct such a search if both of the following conditions are met:

i. The search is for an authorized foreign intelligence or CI purpose and, if directed at a U.S. person, the foreign intelligence sought is significant and the search is not being undertaken to obtain information about the domestic activities of any U.S. person.
ii. The search meets the definition of a physical search in FISA, and satisfies the requirements of FISA for such searches.

4) Only the SecDef, the Deputy SecDef, the USD(I), the Secretary or the Under Secretary of a Military Department, the DIRNSA/CHCSS, the Director, Defense Intelligence Agency (DIA), the Director of the National Geospatial-Intelligence Agency (NGA), or the Director of National Reconnaissance Office (NRO), may seek approval for physical searches in accordance with DoDM 5240.01 Paragraph 3.7.d.(1).

h. PROCEDURE 8: Searches of Mail and the Use of Mail Covers.
1) This procedure governs the physical searches of mail, including the opening or other examination of the content of mail, in the United States and abroad, by a Defense Intelligence Component or anyone acting on its behalf.
2) This procedure also applies to the use of mail covers. A Defense Intelligence Component may only search mail or use a mail cover if such activity is for an authorized FI or CI purpose.

No intelligence unit or activity in the KSNG has the authority to conduct any activities in PROCEDURE 8. Any activity under PROCEDURE 8 without the required mission or authority constitutes a QIA and must be reported immediately.

i. PROCEDURE 9: Physical Surveillance.
1) This procedure governs physical surveillance of any person inside the United States or any U.S. person outside the United States by a Defense Intelligence Component or anyone acting on their behalf. If anyone acting on behalf of a Defense Intelligence Component is conducting physical surveillance, this procedure applies to any devices such person is operating to observe the subject of the surveillance, and not the provisions of PROCEDURE 6.
2) Only CI personnel may conduct physical surveillance with prior approval of the Army Deputy Chief of Staff G-2 or the Commander, U.S Army Intelligence and Security Command (INSCOM).

j. PROCEDURE 10: Undisclosed Participation (UDP) in Organizations. This procedure governs the participation by Defense Intelligence Components and anyone, including sources, acting on behalf of a Component in any organization in the United States or any organization outside the United States that constitutes a U.S. person.
Exclusions. This procedure does not apply to:
1) Personal Participation. Activities conducted within an organization solely for personal purposes (i.e., activities undertaken upon the initiative and at the expense of a person for personal benefit).
2) Voluntarily Provided Information. Activities conducted within an organization by any person who is already a member of the organization, or who joins on his or her own behalf, and later volunteers information to a Defense Intelligence Component not in response to a specific request or Defense Intelligence Component tasking.
3) Publicly Available Information on the Internet. Collection of publicly available information on the Internet in a way that does not require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being.

Unless the UDP is conducted in accordance with DoDM 5240.01 Paragraphs 3.10.e. and f., disclosure of the intelligence affiliation of the person who is acting on behalf of the Defense Intelligence Component will be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization.

k. PROCEDURE 11: Contracting for Goods and Services. This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States.
   1) Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if the contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities.
   2) No contract shall be void or voidable for failure to comply with this procedure.

l. PROCEDURE 12: Provision of Assistance to Law Enforcement Authorities. This procedure applies to the assistance by military intelligence to law enforcement authorities for the purpose of:
   1) Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities.
   2) Protecting DoD employees, information, property, and facilities.
   3) Preventing, detecting, or investigating other violations of law.

   DoD intelligence components may provide the following types of assistance to law enforcement authorities:
   1) Incidentally acquired information reasonably believed to indicate a violation of Federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333.
   2) Incidentally acquired information reasonably believed to indicate a violation of State, local, or foreign law may be provided in accordance with procedures adopted by the Heads of DoD Components.
   3) Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to Enclosure 3 of DoD Directive 5525.5.

m. PROCEDURE 13: Experimentation on Human Subjects for Intelligence Purposes. This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component. This procedure does not apply to experimentation on animal subjects.
   1) DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the SecDef or Deputy SecDef, or the Secretary or Under Secretary of the Army or Air force.

n. PROCEDURE 14: Employee Conduct. This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this SOP and other applicable policy (see Appendix A).
   1) Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 and this SOP. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive Orders, and applicable DoD Directives.

o. PROCEDURE 15: Identifying, Investigating and Reporting Questionable Activities.
   The term questionable activity refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive Order or Presidential directive, including E.O. 12333, or applicable DoD policy, including this SOP.
   1) Individuals should report any questionable or perceived improper intelligence activities regardless of whether U.S. persons were involved or not. (See Paragraph 2-7 for reporting procedures).
   2) Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.

3) Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.
4) To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

UNIT CHAINS OF COMMAND AND/OR ACTIVITY SUPERVISORS WILL NOT TAKE ADVERSE ACTIONS AGAINST ANY INDIVIDUAL REPORTING A QUESTIONABLE OR PERCEIVED IMPROPER INTELLIGENCE ACTIVITY.

2-7. Reporting Violations or Questionable Intelligence Activities (QIA)

a. All unit personnel are required by law to report intelligence activities that may appear to be in violation to this and/or other IO guidance as it relates to questionable activity (see Appendix K). Unit level Soldiers/Airmen reporting to Unit IO Monitor should include the following information:
    a. Description of the questionable activity (What)
    b. Date and time of occurrence (When)
    c. Location of occurrence (Where)
    d. Individual or unit responsible for the questionable activity (Who)
b. Units will report QIA of a serious nature and all significant or highly sensitive (S/HS) matters immediately to the State IG with a copy provided to the JA and the State SIO.
c. Reporting of QIA may be made by any secure means.
d. Oral reports should be documented with a written report as soon as possible thereafter.
e. Individuals must report QIA to the State IG within three (3) days of becoming aware of the QIA.
f. Unit level reporting to higher authorities should reflect the format in Appendix H. Formal reporting can be submitted to any of the following:
    (1) IO Monitors at Battalion, Major Subordinate Command, Units, and/or Wings
    (2) The State Intelligence Oversight Program Mgr-J2 Office (785) 646-1706
    (3) The Judge Advocate General's Office (785) 646-1024
    (4) The State Inspector General (785) 646-1020
    (5) The NGB Inspector General (703) 607-2515
    (6) The Army Inspector General, ATTN: IO Division (703) 697-6698
    (7) The Army General Counsel
g. Reporting of QIA will be investigated to determine facts necessary to assess whether activity is legal and consistent with public policy.
h. An IG Investigation is not required; a Commander's Inquiry or AR 15-6 investigation will suffice.
i. When initial investigation is complete, the investigating command must forward a copy of the final investigation report (with any disciplinary or corrective action taken) to the State IG.
j. The status of investigations exceeding one month in duration must be reported to the State IG every thirty (30) days until complete.
k. Use of the unit chain of command is the preferred reporting channel. However its use is not required. Regardless of reporting channels, **NO ADVERSE ACTIONS WILL BE TAKEN AGAINST ANY PERSON WHO REPORTS A QUESTIONABLE ACTIVITY**.

2-8. Intelligence Oversight Reports

a. Quarterly Reports (Appendix I). All IO Monitors will submit quarterly IO training and inspections conducted during the past quarter along with any violation or questionable activities to the KSNG Inspector General with a copy to the State IO Monitor, ATTN: J-2 Senior Intelligence Officer, NLT than the 1st working day of the new quarter.
    1) The report will include the number of personnel assigned to positions that require IO training and the number of personnel available to attend IO training.

2) IO Monitors will hold multiple training events to ensure all Soldiers receive the required IO training by the end of the fiscal year.
3) The report requires the number of personnel that received initial and annual IO training during the quarter which should be derived from the unit's IO training register (Appendix E). The IO training register will be attached to the IO report as a supporting document.
4) The IO report will contain IO inspections, reports of questionable activities and recommended improvements to the IO program received during the quarter.

b. Annual File Review (Appendix F). In the last quarter (July – September) of the training year, IO monitors will review all electronic/hard copy files and intelligence systems to ensure U.S. persons information not retained in violation of DoDM 5240.01 and DoD 5240.1-R.
   1) This review will include keyword searches of information systems predominately used by intelligence personnel or for intelligence missions.
   2) A memorandum for record (MFR) certifying the review was conducted and no unauthorized U.S. persons information has been retained will be maintained on file in the IO Continuity Binder.
   3) A copy of the MFR will be forwarded to the State IO Monitor with the 4th quarter IO report.

c. Self-Inspection Requirement. IO monitors will perform a self-inspection of their IO program in the final quarter (October – December) of the calendar year if the organization has not been evaluated in the current calendar year by IGs from at least one of the following organizations: ATSD (IO), MACOM, MAJCOM, ARNG, or NGB. An example self-inspection checklist can be found in Appendix D of this SOP. A copy of self-inspection results will be maintained in the IO Continuity Binder.

Appendix A: References

Executive Order 12333, United States Intelligence Activities with Amendments EO 13355 and EO 13470

DoD Directive 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))

DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

DoD Directive 5240.01, Change 1, DoD Intelligence Activities, 27 Aug 2014

DoD Regulation 5240.1-R, Change 1, Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons, 8 Aug 2016

DoD Manual 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities, 8 Aug 2016

DTM 08-052, Change 7, DoD Guidance for Reporting QIA and S/HS Matters, 23 Aug 2016

CNGBI 0700.01 Inspector General Intelligence Oversight, 9 Jun 2013

CNGBI 2000.1, National Guard Intelligence Activities, 24 Jul 2015

CNGBM 2000.01 National Guard Intelligence Activities, 26 Nov 2016

NGR 20-10/ANGI 14-101, NG Inspector General Intelligence Oversight Procedures, 5 Nov 14

AFI 14-104, Oversight of Intelligence Activities, 23 Apr 2012

Air Force Guidance Memorandum to AFI 14-104, Oversight of Intelligence Activities, 29 Sep 16

AR 381-10, U.S. Army Intelligence Activities, 3 may 2007

Appendix B. Sample Intelligence Oversight Monitor Duty Appointment

(Office Symbol) **(date)**

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Intelligence Oversight Monitor Duty Appointment

1. Effective on (date), the following individual is appointed as the Primary (or Alternate) Intelligence Oversight Monitor:

Rank & Name:
Unit of Assignment:

2. Authority: JFHQ-KS SOP 381-10.

3. Purpose: Execute this command's Intelligence Oversight Program IAW JFHQ-KS SOP 381-10 and other applicable laws, regulations, and directives.

4. Period: Until officially relieved or released from appointment or assignment (or exact period, if known).

5. Special Instructions:

a. Provide initial and annual refresher training for all personnel assigned to intelligence activities, all personnel with a core intelligence Military Occupational Specialty (MOS) (or Air Force Specialty Code (AFSC)), and the undersigned.

b. Investigate and correct improper and/or questionable activities as identified.

c. Become familiar with applicable laws, regulations, directives and policies.

(Commander's Name)
(Rank), (Branch), KSNG

DISTRIBUTION:
Commanding
1 – Appointee
1 – Unit of Assignment
1 – BN level S2
1 – BDE level S2
1 – JFHQ-KS J2
1 – State IO Monitor
1 – Inspector General

Appendix C. THE IO CONTINUITY BINDER

The IO Monitor will maintain the unit IO Continuity Binder. The binder may be in electronic or hard copy format and will contain the following, at a minimum:

a. Unit IO SOP
b. Appointment letters for Primary and Alternate IO Monitors
c. IO Monitor duties and responsibilities
d. Unit IO Training
e. IO training records
f. Unit-oriented IO Checklist
g. Self-inspection and inspection records
h. QIA process and report format
i. Copies of any QIA reports
j. Annual file review certification MFR
k. EO 12333 United States Intelligence Activities with Amendments EO 13355 and EO 13470
l. DoDD 5240.01, Change 1, DoD Intelligence Activities, 27 Aug 2014
m. DoDM 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities, 8 Aug 2016
n. DoD 5240.1-R, Change 1, Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons, 8 Aug 2016
o. CNGBI 2000.01 National Guard Intelligence Activities, 24 Jul 2015
p. CNGBM 2000.01 National Guard Intelligence Activities, 26 Nov 2016
q. NGR 20-10/ANGI 14-101 NG Inspector General Intelligence Oversight Procedures, 5 Nov 14
r. KSNG IO SOP, 9 Dec 2016
s. DTM 08-052, Change 7, DoD Guidance For Reporting QIA and S/HS Matters, 23 Aug 2016
t. NGB Guide to Handling Information on US Persons While Operating Within the US
u. DoDI 5200.27 Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense
v. NG-J2 White Paper: Role of National Guard Intelligence During Civil Disturbances
w. CNGBI 0700.01 Inspector General Intelligence Oversight, 9 Jun 2013
x. AR 381-10 US Army Intelligence Activities, 3 May 2007 (Joint Staffs and ARNG units only)
y. AFI 14-104, Oversight of Intelligence Activities, 23 Apr 2012 (Joint Staffs and ANG units only)
z. Air Force Guidance Memorandum to AFI 14-104, Oversight of Intelligence Activities, 29 Sep 16 (Joint Staffs and ANG units only)

Appendix D.

For Use During Oversight and Staff Assistance Visits
Prepared by NGB-IGO
AS OF: 23 SEPTEMBER 2014

ARNG/ANG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
1. Does the unit have an Intelligence Oversight (IO) monitor appointed in writing? - Do assigned personnel know who the command IO monitor is? - Is the appointment letter posted in the work area? - Are IO monitor duties/responsibilities available in writing? - Are IO monitors submitting quarterly IO reports to the State J2?	Y/N	Comments
2. Does the unit have the following (digital copies acceptable): A. Executive Order 12333 B. DoDD 5240.01 (2007) C. DoDD 5240.1-R (1982) D. DTM 08-052 (2013) E. AR 381-10 (2007) F. AFI 14-104 (2014) G. DoDD 5148.11 (2013) H. CNGBI 0700.01 (2013) I. CNGBI and CNGBM 2000.01 (2012) (rescinded NGR 381-10) J. J2/SIO Portion of State SOP K. NGB-IGO GKO Link: https://gkoportal.ng.mil/ngb/STAFF/D01/B02/S03/SitePages/Home.aspx L. ATSD(IO) Link: http://atsdio.defense.gov/Library.aspx		
3. Does the unit have command directives and checklists? Is the unit in compliance with command directives and guidance?		
4. Is the unit's IO program inspected at least annually? (External or Internal) - Are inspection results posted/archived for five years?		
5. Does the unit conduct and document initial Intelligence Oversight training within 90 days of arrival on station? Is the training tailored to the unit mission?		
6. Does the unit conduct and document recurring training at least on an annual basis?		
7. Do assigned personnel understand the obligations to report any Questionable Intelligence Activity (QIA) and Significant or Highly Sensitive (S/HS) Matters under the guidelines of the IO program?		
8. Are assigned personnel aware of the proper procedures and methods for reporting QIA and S/HS matters?		
9. Are files maintained to ensure they do not violate the IO program? How?		
10. Are intelligence products and files reviewed periodically to ensure they are maintained in accordance with the IO program? - Is this review documented (annual file review memo)?		
11. Has the unit expanded the command IO program in any other ways? - If so, how?		
12. Are there any Information Operations Staffs assigned to the command? - If so have they received IO training? - Does it de-conflict intelligence and information operations IAW DoDD 3600.01, paragraph 5.7.4?		

NOTE: This document is not a checklist, but rather a tool for units and sections to utilize for successful IO Program assessment. Remember, a successful IO program is a cognitive process wherein this document builds a foundation for a unit to improve upon.

Appendix E. Intelligence Oversight Training Register

The following individuals received Intelligence Oversight Training on the date indicated.

NAME (Print and sign)	ORGANIZATION	DATE	TRAINER (Print and sign)	Initial/Refresher

Appendix F: Annual File Review MFR Example

OFFICE SYMBOL Date

MEMORANDUM FOR RECORD

SUBJECT: Annual File Review

1. In accordance with paragraph 3c(4) in Enclosure A of CNGBM 2000.01, an annual review of all electronic (to include network portal sites) and hard copy files was conducted on [date] to ensure no U.S. Persons information was retained in violation of Intelligence Oversight policies found in AR 381-10, CNGBI 2000.01, and CNGBM 2000.01.

2. This letter is certifying that this review of all electronic and hard copy files was conducted in and no unauthorized U.S. Persons information identified.

3. Point of contact for this action is the undersigned at (XXX) XXX-XXXX.

FOR THE COMMANDER:

YOUR NAME
1LT, MI, KSNG
Intelligence Oversight Monitor

Questionable Activity Report Format

1. Description of the questionable activity.

2. Date and time of occurrence.

3. Location of occurrence.

4. Individual or unit responsible for the questionable activity.

NO ADVERSE ACTIONS WILL BE TAKEN AGAINST ANY PERSON WHO REPORTS QUESTIONABLE ACTIVITY.

Appendix H. Report of Questionable Intelligence Activity

OFFICE LETTER HEAD DATE

MEMORANDUM FOR Office of the Kansas Inspector General, 2722 Topeka BLVD, Topeka, KS 66611-1287

SUBJECT: Report of Questionable Intelligence Activity

1. I am reporting a questionable intelligence activity of Procedure ____ under Procedure 15 in accordance with DOD 5240.1-R and AR 381-10 or AFI 14-104.

2. Reports will describe the following:

- Identification of the personnel committing the alleged questionable intelligence activity by rank or civilian grade; security clearance and access; unit of assignment, employment, attachment or detail; and assigned duties at the time of the activity. Do not identify individuals by name or other personal identifier unless the TIG or DCS, G2 (DAMI–CDC) so requests.
- When and where the activity occurred.
- A description of the activity and how it constitutes a questionable intelligence activity. The applicable portion(s) of this regulation and other applicable law or policy will be cited.
- Command and/or investigative agency actions planned or ongoing, if applicable.

(Reference to AR 381-10 Chapter 15, Procedure 15, Paragraph 15-2 (c).)

Signature Block

Appendix I: IO Quarterly Report MFR

(Office Symbol) (Date)

MEMORANDUM FOR THE INSPECTOR GENERAL, Kansas National Guard, 2800 SW Topeka Blvd, Topeka, Kansas 66611

SUBJECT: IO Quarterly Report, XX Quarter, FYXX

1. The purpose of this memorandum is to provide the (unit) XX Quarter, FYXX Intelligence Oversight Report.

2. Training and Education. XX personnel received Annual Refresher IO Training, and XX personnel received Initial IO Training. XX personnel current on IO Training of XX personnel required to have IO Training for XX% current on IO Training.

a. Annual Refresher Training.

LAST NAME	FIRST NAME	RANK	DATE (YYYYMMDD)

b. Initial Training.

LAST NAME	FIRST NAME	RANK	DATE (YYYYMMDD)

3. IO Inspections Conducted.

a. IG Inspections. List any IG IO inspections during the quarter.

b. Staff Inspections. List any Staff IO inspections during the quarter.

c. Command Inspections. List any command IO inspections during the quarter.

4. Questionable Activity.

5. Improvement Recommendations for IO.

    a. Recommendation #1.

6. POC is the undersigned at 785-XXX-XXX and your.name.mil@mail.mil.

NAME
RANK, KSNG
Intelligence Oversight Monitor

Appendix J. INTELLIGENCE OVERSIGHT CHECKLIST
COMMAND INSPECTION CHECKLIST (BN/BDE/DIV)

UNIT DESIGNATION AND LOCATION _____

INSPECTION TEAM CHIEF_____DATE_____

C020700 – Intelligence Oversight
References: Executive Order 12333, DoDD 5200.27, DoDD 5240.1, DoD Regulation 5240.1-R, AR 381-10/ AFI 14-104, AR 20-1/ AFI 90-201, AR 1-201, CNGBI 2000.1, CNGBM 2000.01, CNGBI 0700.01, KSNG SOP 381-10

Unit (Major Subordinate Command, Battalion, Air Wing)				
Administrative		**GO**	**NO-GO**	**N/A**
H020701	Has the Commander established and maintained an effective IO program for all personnel assigned or attached to the organization? (CNGBI 2000.01, Encl A, 3a(4))			
H020702	Has the commander ensured MI personnel and non-MI personnel conducting intelligence activities are fully aware of and comply with their individual responsibilities? (AR 381-10, 1-4p(2); AFI 14-104, 4.7; CNGBI 0700.01, Encl A, 1a)			
H020703	Has the Commander appointed, in writing, experienced intelligence professionals to serve as primary and alternate IO Monitors who hold the appropriate security clearances and accesses and who have complete access to all information necessary to carry out responsibilities and has the appointment letter been posted in the general work area? (AR 381-10, 1-4p(4); AFI 14-104, 4.7.4; CNGBI 2000.01, Encl A, 3a(5); CNGBI 0700.01, Encl A, 1a and 1f(1); JFHQ-KS SOP 381-10, 2-1)			

H020704	Has the IO Monitor maintained an IO Continuity Book, electronic and/or hard copy, containing, at a minimum, copies of: applicable regulations and instructions; Standard Operating Procedures (SOP); training materials and documentation; IO Monitor appointment letters; records of IO SAVs and inspections; annual file review certification; self-inspection reports; and Memoranda for Record (MFR)? _____ Appointment letters for Primary and Alternate IO monitors _____ IO monitor duties and responsibilities _____ Unit IO training _____ IO training records (initial, annual, and pre-deployment) _____ Copies of the following IO Reference Documents: _____ Executive Order 12333 *(United States Intelligence Activities)* _____ DoD Directive 5148.11 *(Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))* _____ DoD Directive 5200.27 *(Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense)* _____ DoD Directive 5240.1 (DoD Intelligence Activities) _____ DoD Regulation 5240.1-R, *(Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons)* _____ AR 381-10 (US Army Intelligence Activities)/ AFI 14-104 *(Oversight of Intelligence Activities)* _____ CNGBI 2000.01 *(National Guard Intelligence Activities)* _____ CNGBM 2000.01 *(National Guard Intelligence Activities)* _____ CNGBI 0700.01 *(Inspector General Intelligence Oversight)* _____ JFHQ-KS SOP 381-10 *(Intelligence Oversight Activities)* _____ Unit IO SOP/Memorandum _____ Unit-oriented IO checklist _____ Self-inspection and inspection records			

	_____ QIA process and report format _____ Copies of any QIA reports _____ Annual file review certification MFR _____ Roster of personnel assigned to the intelligence section and personnel with an intelligence MOS/AFSC _____ Intelligence oversight standard briefing and POI _____ Intelligence oversight scenarios _____ Intelligence oversight program helpful information (Frequently Asked Questions, IG Intelligence Oversight User Guide, web site information, helpful ideas) _____ Messages & memoranda related to force protection and intelligence oversight (CNGBI 2000.01, Encl A, 3b(4); CNGBM 2000.01, Encl N; CNGBI 0700.01, Encl A, 1f(2); JFHQ-KS SOP 381-10, 2-3)			
H020705	Has the IO Monitor ensured the State IO policy and applicable references are maintained and available to the organization in hard copy and/or electronic format? (CNGBI 2000.01, Encl A, 3b(5))			
H020706	Has the commander implemented a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files to the Investigative Records Repository or information into intelligence databases? (AR 381-10, 1-4p(5))			
H020707	Has the Commander implemented a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS? (AR 381-10, 1-4p(6))			
H020708	Has the IO Monitor reviewed all intelligence files, electronic and paper, at a minimum of once per calendar year to ensure any USPERs information was retained IAW Procedure 4 of DoD 5240.1-R and certified that all files have been reviewed through MFR, which is maintained on file in the IO Continuity Book? (AR 381-10, 3-3c; CNGBI 2000.01, Encl A, 3b(8); CNGBI 0700.01, Encl A, 1f(7))			
H020709	Have quarterly reports been submitted through the chain of command to the State IG? (CNGBI 0700.01, Encl A, 1a; AFI 14-104, 7.3.1; JFHQ-KS SOP 381-10, 2-5)			
H020710	Do quarterly IO reports minimally include the following? (AR 381-10, 15-6d(3); AFI 14-104, 7.3.2; JFHQ-KS SOP 381-10, App B) *(a)* A description of significant oversight activities undertaken during the quarter. *(b)* Identification of unlawful or improper activities discovered or reported. *(c)* Suggestions for improvement of the oversight system.			
H020711	Have employees, supervisors, IO monitors, and/or Commander reported questionable intelligence activity (QIA) that may violate guiding laws or policies through command or inspector general channels to JFHQ-KS IG and JFHQ-KS JA immediately upon discovery? (AR 381-10, 15-2a; AFI 14-104, 7.1.1; CNGBI 2000.01, Encl A, 3b(9) and 3c(5); CNGBM 2000.01, Encl A, 15c(2); JFHQ-KS SOP 381-10, 4-1)			
Training		**GO**	**NO-GO**	**N/A**
H020712	Is IO training (initial and annual refresher) included in the unit commander's Yearly Training Guidance? (CNGBI 0700.01, Encl A, 1a)			
H020713	Is IO training scheduled on the yearly training schedule and the unit training schedule and documented using the IO training register? (JFHQ-KS SOP 381-10, 2-2e)			

H020714	Has the Commander received IO training? (CNGBI 2000.01, Encl A, 3a(1); AFI 14-104, 4.7.7)			
H020715	Have intelligence personnel completed the organization's IO training within 90 days of assignment/ employment, as well as annual refresher training and pre-deployment training? (CNGBM 2000.01 Encl C, 1b(1); CNGBI 2000.01, Encl A, 3c(4); CNGBI 0700.01, Encl A, 1a and 1f(3); JFHQ-KS SOP 381-10, 2-2b)			
H020716	Have all T-32 personnel with a core intelligence Military Occupational Specialty (MOS) or Air Force Specialty Code (AFSC) regardless of unit mission, duty title, or assignment received IO training? (CNGBM 2000.01 Encl C, 1a(3))			
H020717	Has the IO monitor coordinated with the IG and JA to provide additional training on IO, or other matters affecting intelligence support keyed to organizational missions and responsibilities, specifically Procedures 1 through 4 and 12, 14, and 15? (CNGBM 2000.01 Encl C, 2(a))			
H020718	Has the IO Monitor conducted IO training and maintained records of this training for three calendar years, to include the dates personnel received training? (AFI 14-104, 4.8.1; CNGBI 2000.01, Encl A, 3b(2); CNGBM 2000.01, Encl C, 3)			
H020719	Has the IO monitor provided all personnel refresher IO training at least once every calendar year? (CNGBM 2000.01 Encl C, 1b(2); CNGBI 0700.01, Encl A, 1f(4); KSNG SOP 381-10, 2-2e)			
H020720	Have annual refresher training records been maintained for a period of five years? (CNGBI 0700.01, Encl A, 1f(5); JFHQ-KS SOP 381-10, 2-2i)			
H020721	Has the Commander ensured all personnel assigned or attached to the organization conducting intelligence or intelligence-related activities received required IO training, and know IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions? (AR 381-10, 1-4p(3); AFI 14-104, 4.7.5; CNGBI 2000.01, Encl A, 3a(6))			
H020722	Has the IO Monitor implemented an IO program to educate and train intelligence personnel on applicable IO regulations and directives, as well as individual reporting responsibilities? (CNGBI 2000.01, Encl A, 3b(1); AFI 14-104, 4.8.1)			
H020723	Do the intelligence personnel know the authorized mission of their organization to which assigned? (AFI 14-104, 4.9.1; CNGBI 2000.01, Encl A, 3c(1))			
H020724	Can intelligence personnel identify the organization's IO Monitor and know how to establish contact? (CNGBI 2000.01, Encl A, 3c(6); CNGBI 0700.01, Encl A, 1a)			
H020725	Has the IO Monitor tested personnel to confirm that they can identify, at a minimum, the regulations and instructions governing reporting procedures on QIA and the identity of the IO Monitors? (CNGBI 2000.01, Encl A, 3b(3))			
H020726	Can intelligence personnel identify the contents of Procedures 1-4, 12, 14, and 15 of DoD 5240.1-R, and any other procedures applicable to the assigned unit's mission/discipline, CNGBI 2000.01, and KSSOP 381-10? (CNGBI 2000.01, Encl A, 3c(2); AFI 14-104, 4.9.2)			
Inspections		**GO**	**NO-GO**	**N/A**
H020727	Has the IO Monitor performed a self-inspection in the final quarter of the calendar year, if the organization was not evaluated that year by an IG from one of the following organizations: the Assistant to the Secretary of Defense, Intelligence Oversight; Major Command (Army) or MAJCOM (AF); ARNG; ANG; or NGB? (CNGBI 2000.01, Encl A, 3b(6); CNGBM 2000.01, Encl O, 5; AFI 14- 104, 4.8.3 and 6.2; JFHQ-KS SOP 381-10, 2-4b)			

H020728	Have copies of self-inspection results been maintained in the IO Continuity Binder? (CNGBM 2000.01, Encl O, 5; JFHQ-KS SOP, 2-4a)			
H020729	Does the Organizational Inspection Program (OIP) include intelligence oversight inspections? (AR 1-201, 3-2a; JFHQ-KS SOP 381-10, 2-4a)			
	Counter Drug (CD) *(additional requirements)*	**GO**	**NO-GO**	**N/A**
H020730	Has the intelligence element provided the raw information and resultant analysis to the Civilian Law Enforcement Agency (CLEA) and not retained the data in intelligence files or databases? (AR 381-10, 12-4; CNGBM 2000.01, Encl A, 12e(2); CNGBI 3100.01, Encl B, 6b; JFHQ-KS SOP 381-10, 3-6a)			
H020731	Have requests for support requiring approval under procedure 12 been through the P12 (Procedure 12) Memorandum? (CNGBM 2000.01, Encl A, 12f)			
H020732	Are Memoranda of Understanding maintained on file for a minimum of 2 years stating that supported LEAs are responsible for obtaining legal authorization required to permit information gathering? (0700.01, Encl A, 1i(2); JFHQ-KS SOP 381-10, 3-6b)			
H020733	Has IO training, with an emphasis on the handling, protection, distribution, and destruction of U.S. persons information, been included in doctrinal training given to each member at initial entry and repeated annually for all personnel? (CNGBM 2000.01, Encl D, 4b(2)(a); JFHQ-KS SOP 381-10, 3-6c)			
H020734	Has the PAO consulted with the CD coordinator to determine whether news releases would pose OPSEC issues? (CNGBM 2000.01, Encl E, 10d(1))			
	Civil Support Team (CST) **"Non-DoD Persons Information Protection Program"**	**GO**	**NO-GO**	**N/A**
H020735	Does the WMD-CST have a "Non-DoD Persons Information Program" Primary and Alternate Monitors appointed in writing? (CNGBI 2400.00A, Encl A, 3a(5) and Encl C,1a)			
H020736	Has the CST Commander received Non-DoD Persons Information training? (CNGBI 2400.00A, Encl A, 3a(2))			
H020737	Does the CST maintain a "Non-DoD Persons Information Program" Continuity Binder that contains the following items: _____ Appointment letters for Primary and Alternate Program Monitors. _____ Program Monitor duties and responsibilities. _____ Unit non-DoD Persons information protection training. _____ Program training records (initial and annual). _____ Copies of: _____DoD Directive 5200.27 *(Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense)* _____AR 380-13 *(Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations)* _____CNGBI 2400.00A *(Acquisition and Storage of Information Concerning Persons and Organization not Affiliated with the Department of Defense)* _____ Unit-oriented program self-inspection checklist. _____ Self-inspection and inspection records. _____ Annual file review certification MFR. (CNGBI 2400.00A, Encl A, 3b(5) and Encl C, 1a-h; CNGBI 0700.01, Encl A, 1j(3)(b))			

H020738	Have personnel who acquire, process, retain and disseminate information about persons or organizations not affiliated with DoD been trained within 90 days of assignment and annually thereafter? (CNGBI 2400.00A, Encl A, 3b(2); CNGBI 0700.01, Encl A, 1j(3)(c))			
H020739	Upon completion of operations, has all information or files been redacted of all U.S. persons information before being used in After Action Reports (AARs), Mission Termination Packets, or other follow-up reports? (CNGBM 2000.01, Encl D, 4b(3)(b); CNGBI 0700.01, Encl A, 1j(2); JFHQ-KS SOP 381-10, 3-7b)			
H020740	Does the CST have a unit inspection checklist? (CNGBI 0700.01, Encl A, 1j(3)(a))			
H020741	Has a self-inspection been performed in the final quarter of the calendar year if NGB-IGO has not evaluated the program in the current calendar year? (CNGBI 2400.00A, Encl A, 3b(5))			
H020742	Have all files, electronic and paper, been reviewed at a minimum, once a calendar year to ensure all non-DoD persons information retained is in accordance with CNGBI 2400.00A, and certify that all files have been reviewed through a memorandum for record (MFR), which is maintained on file in the program continuity book? (CNGBI 2400.00A, Encl A, 3b(7))			
JFHQ-KS				
Administrative		**GO**	**NO-GO**	**N/A**
H020743	Has The Adjutant General (TAG) appointed in writing intelligence professionals to be the State intelligence oversight primary and alternate staff officers, and ensure that all intelligence components within the State have an intelligence oversight primary and alternate staff officer? (AR 381-10, 1-4n(2); CNGBI 2000.01, Encl A, 2b(3); JFHQ-KS SOP 381-10, 2-1a)			
H020744	Has the JFHQ-KS generated a P12 Memo and sought approval through NGB-J2 before the execution of a mission? (CNGBM 2000.01, Encl A, 12f)			
H020745	Were Proper Use Memoranda (PUMs) written on the organization letterhead and signed by the organization certifying official, a field grade officer or civilian equivalent? (CNGBM 2000.01, Encl E, 6a(1))			
H020746	Has JFHQ-KS submitted PUMs to NGB-J2 (T-32) or the gaining COCOM, MACOM, or MAJCOM (T-10) before airborne platforms were tasked to collect domestic imagery? (CNGBM 2000.01, Encl E, 3 or 6a(2))			
H020747	Has imagery collected through Remotely Piloted Vehicles (RPVs)/ Unmanned Aircraft Systems (UASs)/ Unmanned Aerial Vehicles (UAVs) been stored without using references to a U.S. persons identifiers and is not retrievable by reference to a U.S. persons identifiers? (CNGBM 2000.01, Encl E, 5a)			
H020748	Has the JFHQ-KS Judge Advocate (JA) reviewed intelligence plans, proposals, and concepts, to include PUMs, for legality and propriety? (CNGBI 2000.01, Encl A, 2d(4))			
H020749	After the conclusion of security operations in support of a Law Enforcement missions, has all non-DoD-affiliated persons' information been purged, destroyed, or provided to the appropriate agency? (CNGBM 2000.01, Encl K, 1g)			
H020750	Do Security, Force Protection (FP), or Law Enforcement (LE) personnel, and not intelligence personnel, lead "information fusion cell" or "threat working group" meetings? (CNGBM 2000.01, Encl K, 1e)			
H020751	Has the PAO consulted with the CD coordinator to determine whether news releases would pose OPSEC issues? (CNGBM 2000.01, Encl E, 10d(1))			

H020752	Has the JFHQ-KS IG submitted quarterly reports to NGB-IO by the 5th day of the month following the end of the quarter? (CNGBI 0700.01, 6b(7)(b))			
Training		**GO**	**NO-GO**	**N/A**
H020753	Has the JFHQ-KS J2 provided a standard intelligence oversight training brief to each unit and intelligence activity? (JFHQ-KS SOP 381-10, 2-2g)			
H020754	Has the JFHQ-KS J2 ensured all personnel assigned or attached to JFHQ-KS J2 received required IO training, and know IO statutory and regulatory guidance, to include reporting responsibilities and all restrictions? (CNGBI 2000.01, Encl A, 2b(4))			
H020755	Has the JFHQ-KS JA trained members of organizations engaged in intelligence and intelligence-related activities on all laws, policies, treaties, and agreements that apply to their activities, as required? (CNGBI 2000.01, Encl A, 2d(5))			
H020756	Have TAG, director J2, IGs, and JAs received IO Training? (CNGBM 2000.01, Encl C, 1a(7))			
H020757	Have all T-32 military and civilian personnel assigned or attached to JFHQ-KS on a permanent or temporary basis, regardless of military specialty or job function, conducting intelligence or intelligence-related activities received IO training? (CNGBM 2000.01, Encl C, 1a(2))			
H020758	Have all T-32 personnel with a core intelligence Military Occupational Specialty (MOS) or Air Force Specialty Code (AFSC) regardless of duty title or assignment assigned to JFHQ-KS received IO training? (CNGBM 2000.01, Encl C, 1a(3))			
H020759	Have all contractors or consultants assigned or attached to JFHQ-KS, if they are involved in T-32 activities subject to the procedures of DoD 5240.1-R, received IO training? (CNGBM 2000.01, Encl C, 1a(4))			
Inspections		**GO**	**NO-GO**	**N/A**
H020760	Does the Organizational Inspection Program (OIP) include intelligence oversight inspections? (AR 1-201, 3-2a and 3-2e)			
H020761	Has the JFHQ-KS IG conducted intelligence oversight inspections of intelligence activities and components within the command as part of the Organizational Inspection Program (OIP) in accordance with EO 12333, DOD 5240.1–R, and AR 381–10? (AR 20-1, 1-4b(3)(a))			
H020762	Have intelligence oversight inspections been accomplished as required? (AR 20-1, 5-3a; AR 381-10, 1-4n(3); AFI 14-104, 6; CNGBI 0700.01, 6b(1))			
H020763	Has the JFHQ-KS IG inspected all assigned intelligence components a minimum of once every 2 years? (AR 20-1, 1-4a(3)(a) and 5-3e; CNGBI 0700.01, 6b(1); JFHQ-KS SOP 381-10, 2-4d)			
H020764	Has the JFHQ-KS IG periodically tested personnel within an intelligence organization to confirm whether they can identify regulations governing reporting procedures on QIA and the identity of the IO Officer? (CNGBI 0700.01, Encl A, 1c; JFHQ-KS SOP 381-10, 2-4d)			
H020765	Has the JFHQ-KS IG forwarded copies of IO related findings/ inspection reports to the NGB-IG office? (CNGBI 0700.01, 6b(8))			

Questionable Intelligence Activities (QIA)		**GO**	**NO-GO**	**N/A**
H020766	Have reports of questionable intelligence activities (QIA) of a serious nature and all Significant/ Highly Sensitive (S/HS) matters been forwarded to the NGB- IG, NGB-JA, or office of the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD (IO))? (AR 381-10, 1-4n(4); CNGBM 2000.01, Encl A, 15c(2); JFHQ-KS SOP 381-10, 4-1b)			
H020767	Has the JFHQ-KS IG reported any QIA to DAIG's Intelligence Oversight Division (SAIG-IO) in accordance with procedure 15, AR 381-10? (AR 20-1, 1-4b(10))			
H020768	Has the JFHQ-KS IG Reported to TIG through DAIG's Intelligence Oversight Division (office symbol SAIG–IO) within 2 working days by secure means any inspector general action request (IGAR) containing an allegation against any person assigned to a Special Access Program (SAP) or sensitive activity as defined in AR 380–381? (AR 20-1, 1-4b5(e))			
INTELLIGENCE OVERSIGHT Totals:				

COMMENTS:

Appendix K. QIA and Significant/Highly Sensitive Matters Flow Chart