Adjutant General's Department
Headquarters, Kansas National Guard
5920 SE Coyote Drive
Topeka, Kansas 66619
08 February 2019

KSNG SOP 381-10

Kansas National Guard Intelligence Oversight Standard Operating Procedures

By order of the Adjutant General:

MURDOCK.ROGER.DEAN.1149154767 Digitally signed by MURDOCK.ROGER.DEAN.1149154767 Date: 2019.03.08 17:33:59 -06'00'

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

Official:

Digitally signed by HARRIMAN.CHARLES.ROY.1150798554 Date: 2019.03.12 20:10:51 -05'00'

CHARLES R. HARRIMAN
LTC, KSNG
J2, Director of Intelligence

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 08 December 2016

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 CNGBI 2000.1C, Dodd 5148.13, 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 Manual 5240.01.
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 Manual 5240.01.

1-5. References
Required Intelligence Oversight 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. JFHQ-KS 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 JFHQ-KS 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 and 12, employee conduct, reporting QIA and S/HSM), 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, employee conduct, reporting QIA and S/HSM). 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 JFHQ-KS IO monitor.
i. Units will document annual intelligence file reviews through a Memorandum for Record (MFR) (Appendix F).
j. All individuals assigned as an IO monitor or IO alternate must complete the IO Monitor Certification Course on Guard University within 90 days of being assigned, then provide the training certificate to the JFHQ-KS IO monitor. The course requires CAC access and can be found at: https://guardu.ellc.learn.army.mil/webapps/blackboard/execute/enrollCourse?context=INMENU&course_id=_57903_1.

2-3. Compliance Inspections

a. The IG will conduct compliance inspections IAW the OIP checklist in Appendix J after being directed by the directing authority (The Adjutant General) the conduct the inspection.
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 Manual 5240.01.
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 CNGBI 2000.1C and CNGBM 2000.01, 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, or remotely piloted aircraft (RPA) 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. Note: KSNG Soldiers and Airmen are not authorized to use commercial off-the-shelf (COTS) UAS, such as Quad copters.
d. PUM. Requests for a PUM should be submitted through the JFHQ-KS IO monitor at 785-646-0201. Current NG Domestic Imagery policy requires that an approved PUM **MUST** be on file **PRIOR** to any

airborne domestic imagery collection mission. Conducting an airborne domestic imagery collection mission **WITHOUT** an approved PUM on file is a **QUESTIONABLE INTELLIGENCE ACTIVITY** which **MUST** be reported through IO channels. The **ONLY** exception to this policy is **IMMEDIATE RESPONSE AUTHORITY**. If you need to collect airborne domestic imagery in order to save lives, mitigate damage, etc, then fly the mission and submit the PUM **IMMEDIATELY** afterwards. A draft PUM template is available in Annex L. If you require a different type of PUM contact the JFHQ-KS IO monitor for a different example.

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, employee conduct, reporting QIA and S/HSM.

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 if necessary.

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 delegate 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: DoD 5240.1-R Change 2, 26 Apr 17 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: DoD 5240.1-R Change 2, 26 Apr 17 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: DoD 5240.1-R Change 2, 26 Apr 17 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. Employee Conduct. (Formerly PROCEDURE 14) DoDD 5148.13, 26 Apr 17 National Guard intelligence components must: Conduct intelligence activities IAW all relevant executive orders, law, regulations, policies and this SOP. Be familiar with Procedures 1-4 (DoDM 5240.01), employee conduct, reporting QIA, S/HSM and Federal Crimes (information formerly known as Procedures 14-15 of DoD 5240.1-R), and any other procedures employed by the intelligence component. They should conduct initial and annual training for Intelligence Oversight Civil liberties and privacy protection.

o. Identifying, Investigating, and Reporting Questionable Activities and Significant/Highly Sensitive Matters (S/HSM) (formerly PROCEDURE 15) DoDD 5148.13, 26 Apr 17 The term questionable activity refers to any conduct that constitutes, or is related to, an intelligence activity or personnel that may violate the law, any Executive Order or Presidential directive, including E.O. 12333, or applicable DoD policy, including this SOP. Significant/Highly Sensitive Matters (S/HSM): Any development or circumstance involving an intelligence activity or personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Report these matters immediately through chain of command to KSNG IG who reports to Senior DoD Intelligence Oversight Official. Each report of a QIA or S/HSM will be investigated to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies. See Annex G and H.

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

2-7. Reporting Violations, Questionable Intelligence Activities (QIA) or Significant/Highly Sensitive Matters (S/HSM)

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:
    1) Description of the questionable activity (What)
    2) Date and time of occurrence (When)
    3) Location of occurrence (Where)
    4) 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 JFHQ-KS IG with a copy provided to the JA and the JFHQ-KS 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 JFHQ-KS 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 JFHQ-KS Intelligence Oversight Program Mgr-J2 Office (785) 646-0201
    3) The Judge Advocate General's Office (785) 646-0050
    4) The JFHQ-KS Inspector General (785) 646-0020
    5) The NGB Inspector General (703) 607-2511

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 JFHQ-KS IG.
j. The status of investigations exceeding one month in duration must be reported to the JFHQ-KS 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.

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 JFHQ-KS IO Monitor, ATTN: J-2 Senior Intelligence Officer, who will consolidate all reports and forward them to the KSNG Inspector General, NLT than the 3rd working day of the new quarter. (All Quarterly Reports MUST be dated after the end of the quarter being reported.)
    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 JFHQ-KS 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

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

B. DoD Directive 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) 24 Apr 2013

B.1 Re-delegation of Intelligence Oversight Authorities

C. DOD DIRECTIVE 5148.13 Intelligence Oversight April 26, 2017

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

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

F. DoD Regulation 5240.1-R, Change 2, Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons, 26 April 2017

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

G.1 DoD Manual 5240.01 Implementing Guidance for Intelligence Oversight 15 AUG 2016

G.2 DA-G2 DoDD 5148.13 Implementation Memo 8 December 2017)

G.2.A Enclosure 2 DoDD 5148.13 Implementation Memo 8 December 2017

H. AFI 14-104, Oversight of Intelligence Activities, 5 Nov 2014 with AFGM 4 Oct 2018

I. CNGBI 2000.1C, National Guard Intelligence Activities, 14 August 2018

J. CNGBM 2000.01 National Guard Intelligence Activities, 26 Nov 2012

K. CNGBI 0700.01A Inspector General Intelligence Oversight, 21 December 2018

L. DOJ-DOD MOU 95-04931 Reporting Federal Crimes

M. NGBI 7500.00 Domestic Use of National Guard Unmanned Aircraft Systems 13 October 2016

Non DoD Persons Info Protection Program

A. DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense 7 Jan 1980

B. AR 380-13 Non-Affiliated Persons 30 Sep 1974

C. CNGBI 2400.00 Acquisition and Storage of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense _14 August 2013

D. CNGBI 700.01 Inspector General Intelligence Oversight 9 Jun 2013

E. CNBGI 3501.00 WMD-CST 8July 2014

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 – JFHQ-KS 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. KSNG IO SOP, 8 Feb 2019
l. EO 12333 United States Intelligence Activities with Amendments EO 13355 and EO 13470
m. DoDD 5240.01, Change 1, DoD Intelligence Activities, 27 Aug 2014
n. DoDM 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities, 8 Aug 2016
o. DoD 5240.1-R, Change 2, Procedures Governing the Activities of DoD Intelligence Components That Affect US Persons, 26 April 2017
p. CNGBI 2000.1C, National Guard Intelligence Activities, 14 August 2018
q. CNGBM 2000.01 National Guard Intelligence Activities, 26 Nov 2012
r. CNGBI 0700.01A Inspector General Intelligence Oversight, 21 December 2018
s. AR 381-10 US Army Intelligence Activities, 3 May 2007 (Joint Staffs and ARNG units only)
t. AFI 14-104, Oversight of Intelligence Activities, 5 Nov 2014 with AFGM 4 Oct 2018 (Joint Staffs and ANG units only)
u. DoD Directive 5148.11, Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) 24 Apr 2013
v. DOD DIRECTIVE 5148.13 Intelligence Oversight April 26, 2017
w. DA-G2 DoDD 5148.13 Implementation Memo 8 December 2017
x. Enclosure 2 DoDD 5148.13 Implementation Memo 8 December 2017
y. DOJ-DOD MOU 95-04931 Reporting Federal Crimes
z. NGBI 7500.00 Domestic Use of National Guard Unmanned Aircraft Systems 13 October 2016
aa. DoDD 5200.27 Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense
bb. AR 380-13 Non-Affiliated Persons 30 Sep 1974
cc. CNGBI 2400.00 Acquisition and Storage of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense _14 August 2013
dd. CNGBI 700.01 Inspector General Intelligence Oversight 9 Jun 2013

Appendix D

UNIT: _____ DATE:_____

UNIT POC: _____ REVIEWER:_____

ARNG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
1. Is the Unit Commander, Director or SIO knowledgeable of the missions, plans, and capabilities of subordinate intelligence and intelligence-related units and does he/she levy tasks and missions IAW IO applicable law, policy and guidance? (CNGBI 2000.01, Enclosure A, Para. 14.b.)	**Y/N**	**Comments**
2. Has the Unit Commander, Director or SIO established and maintained an effective Intelligence Oversight program for all personnel assigned or attached to the organization? (CNGBI 2000.01, Enclosure A, Para. 14.c.)		
3. Has Unit Commander, Director or SIO appointed, in writing, experienced intelligence professionals to serve as primary and alternate IO Monitors? (CNGBI 2000.01, Enclosure A, Para 14.d.)		
4. Are copies of the IO Monitor appointment letter posted in the organization's workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 14.d.)		
5. Are all personnel able to identify the organization's IO Monitor and know how to establish contact? (CNGBI 2000.01, Enclosure A, Para. 16.f. and Para 15.b.)		
6. Does the Unit Commander, Director or SIO forward proposals for intelligence activities that may be questionable or contrary to policy to a Service JA and NG-JFHQsState JA for review and submission to NGB-JA if required? (CNGBI 2000.01, Enclosure A. Para. 14.g.)		
7. Has the IO Monitor implemented an IO program that educates and trains intelligence personnel on applicable IO regulations and directives, as well as individual reporting responsibilities? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
8. Is initial IO training provided to all personnel assigned or attached to the unit within 90 days of assignment or arrival? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 14.a., Para. 14.e. and Para. 16.d., CNGBM 2000.01, Enclosure C, Para. 1.(b)(1)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, Para. 15.c.)		

9. Is annual IO refresher training provided to all personnel assigned or attached to the unit? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 14.a., Para. 14.e., CNGBM 2000.01, Enclosure C, Para. 1.(b)(2)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, Para. 15.c.)		
10. Have all personnel assigned or attached to the organization who access or use USPI trained annually on the civil liberties and privacy protections that apply to such information? (CNGBI 2000.01, Enclosure A, para. 14.f.)		

ARNG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
11. Are all personnel able to identify the purpose of the IO Program, the regulations and instructions governing IO, and IO rules impacting their mission? (CNGBI 2000.01, Enclosure A, Para. 16.f. and Para 15.b.)		
12. Are all electronic and hard copy intelligence files at least once each calendar year IAW to ensure that no unauthorized USPI has been retained? (CNGBI 2000.01, Enclosure A, Para. 14.j. and Para. 15.h., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
13. Is a memorandum for record (MFR) certifying the review was conducted and no unauthorized U.S. person information (USPI) has been retained, maintained in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 14.k., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
14. Has the unit submitted a Quarterly IO Report to the JFHQ-State? (CNGBI 2000.01, Enclosure A, Para. 14.l. and Para. 15.j., CNGBI 0700.01, Para. 6.b.(7)(b) and Enclosure A, Para.1.a.)		
15. Has the IO Monitor confirmed that personnel can identify, at a minimum, the purpose of the IO Program, the regulations and instructions governing IO, IO rules impacting their mission, reporting procedures for QIA, S/HS matters and Federal crimes, and the identity of the IO Monitors. ? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
16. Does the IO Monitor maintain an IO Continuity Binder? (CNGBI 2000.01, Para. 15.d. and CNGBM 2000.01 Enclosure N)		

ARNG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
17. Does the IO Continuity Book contain the following? (CNGBI 2000.01, Enclosure A, Para. 15.e.) A. Appointment letters for Primary and Alternate IO Monitors (CNGBM 2000.01, Enclosure N, Para. 1) B. IO Monitor duties and responsibilities (CNGBM 2000.01, Enclosure N, Para. 2) C. Unit IO Training (CNGBM 2000.01, Enclosure N, Para. 3) D. IO training records (initial and annual) (CNGBM 2000.01, Enclosure N, Para. 4) E. Copies of the following IO reference documents: (CNGBM 2000.01, Enclosure N, Para.5) 1) Executive Order 12333 2) DoDD 5148.11 3) DoDD 5148.13 4) DoDD 5240.01 5) DoDM 5240.01 6) DoDD 5240.1-R, Change 2 7) AR381-10 with DA G2 Implementing New IO Policy) 8) CNGBI 2000.01 9) CNGBM 2000.01 10) CNGBI 0700.01 11) State IO SOP, if applicable F. Unit-Oriented IO Checklist (CNGBM 2000.01, Enclosure N, Para. 6) G. QIA, S/HSM and Federal crime reporting process and report format (CNGBM 2000.01, Enclosure N, Para. 7) H. Copies of any QIA, S/HSM and Federal crime reports (CNGBM 2000.01, Enclosure N, Para. 3) I. Annual file review certification MFR		
18. 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 DoD Senior Intelligence Oversight Official, Major Command (Army) or NGB? (CNGBI 2000.01, Enclosure A, Para. 15.f.)		
19. Does the IO Monitor assist in making determinations on collectability of USPI within the five- and 25-year window, as detailed in Procedure 2 of CNGBN 2000.01, and seek assistance from the unit, State JA, NGB-IG, or NG-J2, when required/necessary? (CNGBI 2000.01, Enclosure A, Para. 15.g.)		
20. Are all personnel familiar with reporting procedures for QIA, S/HSM and Federal crimes? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		

21. Is any intelligence activity that may violate guiding laws or policies (QIA) as well as S/HSM and Federal crimes reported immediately upon discovery (CNGBI 2000.01, Enclosure A, Para. 15.i. and Para. 16.e.)		
ARNG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
22. Does the Unit Commander, Director or SIO protect all personnel who report QIA or S/HSM allegations from reprisal or retaliation and report any threats of retaliation to the IG? (CNGBI 2000.01, Enclosure A. Para. 14.h.)		
23. Do all personnel assigned to the JFHQ-State J2 understand their authorized mission? (CNGBI 2000.01, Enclosure A. Para. 16.a.)		
24. Are all personnel assigned to the unit familiar with Procedures 1-4, 12, employee conduct, reporting QIA and S/HSM of references a, b and g, any other procedures applicable to the assigned unit's mission or discipline, this instruction, and any organization-specific regulation, instruction, or standard operating procedures concerning the intelligence mission or discipline? (CNGBI 2000.01, Enclosure A. Para. 16.b.)		
25. Are all intelligence activities conducted IAW applicable law and policy, including DoDM 5240.01, DoDD 5148.13, DoD 5240.1-R Change 2, CNGBI/M 2000.01; and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGBI 2000.01, Enclosure A, Para. 16.c.)		
26. Does the Unit Commander, Director or SIO impose appropriate sanctions upon any employees who violate the provisions of CNGBI/M 2000.01 and other applicable policies? (CNGBI 2000.01, Enclosure A, Para.14.i.)		
27. Has the unit expanded the State IO program in any other ways? If so, how?		

UNIT: _____ DATE:_____

UNIT POC: _____ REVIEWER:_____

ANG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
1. Is the Unit Commander, Director or SIO knowledgeable of the missions, plans, and capabilities of subordinate intelligence and intelligence-related units and does he/she levy tasks and missions IAW IO applicable law, policy and guidance? (CNGBI 2000.01, Enclosure A, Para. 14.b.)	**Y/N**	**Comments**
2. Has the Unit Commander, Director or SIO established and maintained an effective Intelligence Oversight program for all personnel assigned or attached to the organization? (CNGBI 2000.01, Enclosure A, Para. 14.c.)		
3. Has Unit Commander, Director or SIO appointed, in writing, experienced intelligence professionals to serve as primary and alternate IO Monitors? (CNGBI 2000.01, Enclosure A, Para 14.d.)		
4. Are copies of the IO Monitor appointment letter posted in the organization's workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 14.d.)		
5. Are all personnel able to identify the organization's IO Monitor and know how to establish contact? (CNGBI 2000.01, Enclosure A, Para. 16.f. and Para 15.b.)		
6. Does the Unit Commander, Director or SIO forward proposals for intelligence activities that may be questionable or contrary to policy to a Service JA and NG-JFHQsState JA for review and submission to NGB-JA if required? (CNGBI 2000.01, Enclosure A. Para. 14.g.)		
7. Has the IO Monitor implemented an IO program that educates and trains intelligence personnel on applicable IO regulations and directives, as well as individual reporting responsibilities? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
8. Is initial IO training provided to all personnel assigned or attached to the unit within 90 days of assignment or arrival? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 14.a., Para. 14.e. and Para. 16.d., CNGBM 2000.01, Enclosure C, Para. 1.(b)(1)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, Para. 15.c.)		

9. Is annual IO refresher training provided to all personnel assigned or attached to the unit? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 14.a., Para. 14.e., CNGBM 2000.01, Enclosure C, Para. 1.(b)(2)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, Para. 15.c.)		
10. Have all personnel assigned or attached to the organization who access or use USPI trained annually on the civil liberties and privacy protections that apply to such information? (CNGBI 2000.01, Enclosure A, para. 14.f.)		

ANG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
11. Are all personnel able to identify the purpose of the IO Program, the regulations and instructions governing IO, and IO rules impacting their mission? (CNGBI 2000.01, Enclosure A, Para. 16.f. and Para 15.b.)		
12. Are all electronic and hard copy intelligence files at least once each calendar year IAW to ensure that no unauthorized USPI has been retained? (CNGBI 2000.01, Enclosure A, Para. 14.j. and Para. 15.h., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
13. Is a memorandum for record (MFR) certifying the review was conducted and no unauthorized U.S. person information (USPI) has been retained, maintained in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 14.k., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
14. Has the unit submitted a Quarterly IO Report to the JFHQ-State? Is a copy provided to the gaining MAJCOM? (CNGBI 2000.01, Enclosure A, Para. 14.l. and Para. 15.j., CNGBI 0700.01, Para. 6.b.(7)(b) and Enclosure A, Para.1.a.)		
15. Has the IO Monitor confirmed that personnel can identify, at a minimum, the purpose of the IO Program, the regulations and instructions governing IO, IO rules impacting their mission, reporting procedures for QIA, S/HS matters and Federal crimes, and the identity of the IO Monitors. ? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
16. Does the IO Monitor maintain an IO Continuity Binder? (CNGBI 2000.01, Para. 15.d. and CNGBM 2000.01 Enclosure N)		

ANG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
17. Does the IO Continuity Book contain the following? (CNGBI 2000.01, Enclosure A, Para. 15.e.) A. Appointment letters for Primary and Alternate IO Monitors (CNGBM 2000.01, Enclosure N, Para. 1) B. IO Monitor duties and responsibilities (CNGBM 2000.01, Enclosure N, Para. 2) C. Unit IO Training (CNGBM 2000.01, Enclosure N, Para. 3) D. IO training records (initial and annual) (CNGBM 2000.01, Enclosure N, Para. 4) E. Copies of the following IO reference documents: (CNGBM 2000.01, Enclosure N, Para.5) 1) Executive Order 12333 2) DoDD 5148.11 3) DoDD 5148.13 4) DoDD 5240.01 5) DoDM 5240.01 6) DoDD 5240.1-R, Change 2 7) AFI 14-104 with AFGM Implementing New IO Policy) 8) CNGBI 2000.01 9) CNGBM 2000.01 10) CNGBI 0700.01 11) State IO SOP, if applicable F. Unit-Oriented IO Checklist (CNGBM 2000.01, Enclosure N, Para. 6) G. QIA, S/HSM and Federal crime reporting process and report format (CNGBM 2000.01, Enclosure N, Para. 7) H. Copies of any QIA, S/HSM and Federal crime reports (CNGBM 2000.01, Enclosure N, Para. 3) I. Annual file review certification MFR		
18. 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 DoD Senior Intelligence Oversight Official, MAJCOM, or NGB? (CNGBI 2000.01, Enclosure A, Para. 15.f.)		
19. Does the IO Monitor assist in making determinations on collectability of USPI within the five- and 25-year window, as detailed in Procedure 2 of CNGBN 2000.01, and seek assistance from the unit, State JA, NGB-IG, or NG-J2, when required/necessary? (CNGBI 2000.01, Enclosure A, Para. 15.g.)		
20. Are all personnel familiar with reporting procedures for QIA, S/HSM and Federal crimes? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
21. Is any intelligence activity that may violate guiding laws or policies (QIA) as well as S/HSM and Federal crimes reported immediately upon discovery (CNGBI 2000.01, Enclosure A, Para. 15.i. and Para. 16.e.)		

ANG UNIT INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
22. Does the Unit Commander, Director or SIO protect all personnel who report QIA or S/HSM allegations from reprisal or retaliation and report any threats of retaliation to the IG? (CNGBI 2000.01, Enclosure A. Para. 14.h.)		
23. Do all personnel assigned to the JFHQ-State J2 understand their authorized mission? (CNGBI 2000.01, Enclosure A. Para. 16.a.)		
24. Are all personnel assigned to the unit familiar with Procedures 1-4, 12, employee conduct, reporting QIA and S/HSM of references a, b and g, any other procedures applicable to the assigned unit's mission or discipline, this instruction, and any organization-specific regulation, instruction, or standard operating procedures concerning the intelligence mission or discipline? (CNGBI 2000.01, Enclosure A. Para. 16.b.)		
25. Are all intelligence activities conducted IAW applicable law and policy, including DoDM 5240.01, DoDD 5148.13, DoD 5240.1-R Change 2, CNGBI/M 2000.01; and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGBI 2000.01, Enclosure A, Para. 16.c.)		
26. Does the Unit Commander, Director or SIO impose appropriate sanctions upon any employees who violate the provisions of CNGBI/M 2000.01 and other applicable policies? (CNGBI 2000.01, Enclosure A, Para.14.i.)		
27. Has the unit expanded the IO program in any other ways? If so, how?		

UNIT: _____ DATE:_____

UNIT POC: _____ REVIEWER:_____

JFHQ-STATE J2 INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
1. Is the JFHQ-State J2 knowledgeable of all State intelligence, intelligence-related and information operations activities? (CNGBI 2000.01, Enclosure A, Para. 11.a.)	**Y/N**	**Comments**
2. Has the JFHQ-State J2 established and maintained an effective Intelligence Oversight program for all personnel assigned or attached to the JFHQ-State J2? (CNGBI 2000.01, Enclosure A, Para. 11.d.)		
3. Has The Adjutant General (TAG) or JFHQ-State J2 appointed, in writing, experienced intelligence professionals to serve as JFHQ-State primary and alternate IO Monitors? (CNGBI 2000.01, Enclosure A, Para 10.b. and Para. 11.e.)		
4. Are copies of the IO Monitor appointment letter posted in the JFHQ-State J2 workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 11.e.)		
5. Are all JFHQ-State J2 personnel able to identify the organization's IO Monitor and know how to establish contact? (CNGBI 2000.01, Enclosure A, Para. 16.f. and 15.b.)		
6. Is initial IO training provided to all personnel assigned or attached to the JFHQ-State J2 within 90 days of assignment or arrival? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 11.f. and Para. 16.d., CNGBM 2000.01, Enclosure C, Para. 1.(b)(1)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, Para. 15.c.)		
7. Is annual IO refresher training provided to all personnel assigned or attached to the JFHQ-State J2? Is the training tailored to the J2 mission? (CNGBI 2000.01, Enclosure A, Para. 11.f., CNGBM 2000.01, Enclosure C, Para. 1.(b)(2)) Is this training documented in IO training records that are maintained for five years? (CNGBI 2000.01, Enclosure A, P 11 b)		
8. Have all personnel assigned or attached to the JFHQs-State J2 who access or use USPI trained annually on the civil liberties and privacy protections that apply to such information? (CNGBI 2000.01, Enclosure A, para. 11.g.)		
9. Has the JFHQ-State J2 identified all intelligence staffs, units, and personnel performing intelligence and intelligence-related functions within the State, and verified compliance with appropriate directives? (CNGBI 2000.01, Enclosure A, Para. 11.h.)		
10. Does the JFHQ-State J2 advise TAG or the Commanding General (CG) and his or her staff on matters related to the oversight of intelligence and intelligence-related activities and correspond with TAG or the CG regarding the State IO program? (CNGBI 2000.01, Enclosure A, Para. 11.i.)		

11. Does the JFHQ-State J2 coordinate with the State Judge Advocate (JA) and Inspector General (IG) on IO matters? (CNGBI 2000.01, Enclosure A, Para. 11.j.)		

JFHQ-STATE J2 INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
12. Does the JFHQ-State J2 review, in consultation with the JFHQ-State IG, JA, and J3 any planned or on-going NG information-collection activities and submit any required documentation? (CNGBI 2000.01, Enclosure A, Para. 11.k.)		
13. Does the JFHQ-State J2 submit, after consultation with the JFHQ-State JA, a PUM to NGB J2 for any domestic imagery training, exercise, or real-world mission flown in a T32 status? (CNGBI 2000.01, Enclosure A, Para. 11.l., CNGBM 2000.01, Enclosure E, Para. 3)		
14. Are all electronic and hard copy files at least once each calendar year IAW to ensure that no unauthorized USPI has been retained? (CNGBI 2000.01, Enclosure A, Para. 11.m. and Para 15.h., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
15. Has the JFHQ-State maintained on file in the IO Continuity Binder a memorandum for record (MFR) certifying the review was conducted and no unauthorized U.S. person information (USPI) has been retained? (CNGBI 2000.01, Enclosure A, Para. 11.m., CNGBM 2000.01, Enclosure A, Para. 3.c. (4))		
16. Has the JFHQ-State J2 certified the proper use of all domestic commercial or publicly available imagery, such as USGS imagery, Google Earth imagery, and Falcon View imagery, through an internal MFR at least once each calendar year and maintained the MFR on file in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 11.n., CNGBM 2000.01, Enclosure E, Para. 4.)		
17. Has the JFHQ-State J2 submitted a Quarterly IO Report to the JFHQ-State IG for all intelligence organizations, units and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities? (CNGBI 2000.01, Enclosure A, Para. 11.o. and Para. 15.j., CNGBI 0700.01, Para. 6.b.(7)(b) and Enclosure A, Para.1.a.)		
18. Has the JFHQ-State J2 IO Monitor confirmed that personnel can identify, at a minimum, the purpose of the IO Program, the regulations and instructions governing IO, IO rules impacting their mission, reporting procedures for QIA, S/HS matters and Federal crimes, and the identity of the IO Monitors. ? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		

19. Has the State developed and published State IO policy and procedures that include: (1) internal procedures for determining if any USPI may be retained, recording the reasons for retaining USPI, and the authority for approving retention of USPI, (2) purging or redacting information that may not be retained, (3) marking all files containing USPI, and (4) conducting a yearly intelligence file review and certification to ensure that no unauthorized USPI has been retained((CNGBI 2000.01, Enclosure A, Para. 10.c.)		
20. Does the JFHQ-State J2 IO Monitor maintain an IO Continuity Binder? (CNGBI 2000.01, Para. 15.d. and CNGBM 2000.01 Enclosure N)		

JFHQ-STATE J2 INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
21. Does the IO Continuity Book contain the following? (CNGBI 2000.01, Enclosure A, Para. 15.d. and Para 15.e.) A. Appointment letters for Primary and Alternate IO Monitors (CNGBM 2000.01, Enclosure N, Para. 1) B. IO Monitor duties and responsibilities (CNGBM 2000.01, Enclosure N, Para. 2) C. Unit IO Training (CNGBM 2000.01, Enclosure N, Para. 3) D. IO training records (initial and annual) (CNGBM 2000.01, Enclosure N, Para. 4) E. Copies of the following IO reference documents: (CNGBM 2000.01, Enclosure N, Para.5) 1) Executive Order 12333 2) DoDD 5148.11 3) DoDD 5148.13 4) DoDD 5240.01 5) DoDM 5240.01 6) DoDD 5240.1-R, Change 2 7) AR 381-10 with DA-G2 Memo Implementing Guidance for IO 8) AFI 14-104 with AFGM Implementing New IO Policy) 9) CNGBI 2000.01 10) CNGBM 2000.01 11) CNGBI 0700.01 12) State IO SOP, if applicable F. Unit-Oriented IO Checklist (CNGBM 2000.01, Enclosure N, Para. 6) G. QIA, S/HSM and Federal crime reporting process and report format (CNGBM 2000.01, Enclosure N, Para. 7) H. Copies of any QIA, S/HSM and Federal crime reports (CNGBM 2000.01, Enclosure N, Para. 3) I. Annual file review certification MFR		

22. Has the JFHQ-State J2 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 DoD Senior Intelligence Oversight Official, Major Command (Army) or MAJCOM (AF), or NGB? (CNGBI 2000.01, Enclosure A, Para. 15.f.)		
23. Does the JFHQ-State J2 IO Monitor assist in making determinations on collectability of USPI within the five- and 25-year window, as detailed in Procedure 2 of CNGBN 2000.01, and seek assistance from the unit, State JA, NGB-IG, or NG-J2, when required/necessary? (CNGBI 2000.01, Enclosure A, Para. 15.g.)		
24. Are all personnel familiar with reporting procedures for QIA, S/HSM and Federal crimes? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		
25. Is any intelligence activity that may violate guiding laws or policies (QIA) as well as S/HSM and Federal crimes reported to the Attorney General of the U.S. reported immediately upon discovery (CNGBI 2000.01, Enclosure A, Para. 15.i. and Para16.e.)		
26. Do all personnel assigned to the JFHQ-State J2 understand their authorized mission? (CNGBI 2000.01, Enclosure A. Para. 16.a.)		
JFHQ-STATE J2 INTELLIGENCE OVERSIGHT SELF-ASSESSMENT		
27. Are all personnel assigned to the JFHQ-State J2 familiar with Procedures 1-4, 12, 14, and 15 of references a, b and g, any other procedures applicable to the assigned unit's mission or discipline, this instruction, and any organization specific regulation, instruction, or standard operating procedures concerning the intelligence mission or discipline? (CNGBI 2000.01, Enclosure A. Para. 16.b.)		
28. Are all JFHQ-State intelligence activities conducted IAW applicable law and policy, including DoDM 5240.01, DoDD 5148.13, DoD 5240.1-R Change 2, CNGBI/M 2000.01; and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGBI 2000.01, Enclosure A, Para. 16.c.)		
29. Has the JFHQ-J2 expanded the State IO program in any other ways? If so, how?		

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 or

OFFICE LETTER HEAD DATE

MEMORANDUM FOR Office of the Kansas National Guard Inspector General, 2722 SW Topeka Blvd , Topeka, KS 66611-1287

SUBJECT: Report of Questionable Intelligence Activity or significant or highly sensitive matters (S/HSMs)

1. I am reporting a questionable intelligence activity of Procedure ____ or significant or highly sensitive matters (S/HSMs) in accordance with DoDD 5148.13, DOD 5240.1-R and AR 381-10 or AFI 14-104.

2. Reports will describe the following:

- A narrative describing the incident.
- A statement describing when the incident occurred, when it was initially reported within the KSNG, and when it was reported to the KSNG IG; if applicable, explain any delay in reporting.
- An explanation of why the incident is considered a QIA or S/HSM, if so reported. For each QIA, identify the specific law, E.O., Presidential directive, Intelligence Community Directive, or applicable DoD policy that was violated. For each S/HSM, explain why the incident could impugn the reputation of the Intelligence Community or otherwise call into question the propriety of intelligence activities.
- An analysis of how or why the incident occurred, identifying the root cause.
- An assessment of the anticipated impact of the reported incident on national security or international relations, as well as any mitigation efforts, including success and failures of such efforts. If there has been no impact or if no impact is anticipated, the report should state this.
- An assessment of any impact the reported incident may have on civil liberties or privacy rights.
- The remedial action taken or planned to prevent recurrence of the incident. Include a description of actions taken if the incident concerns information (including U.S. person information) improperly acquired, handled, used, disseminated, or destroyed.
- An indication of whether the incident is open or closed. If open, provide the status of the ongoing investigation. If closed, indicate whether any allegations were substantiated or not substantiated.

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

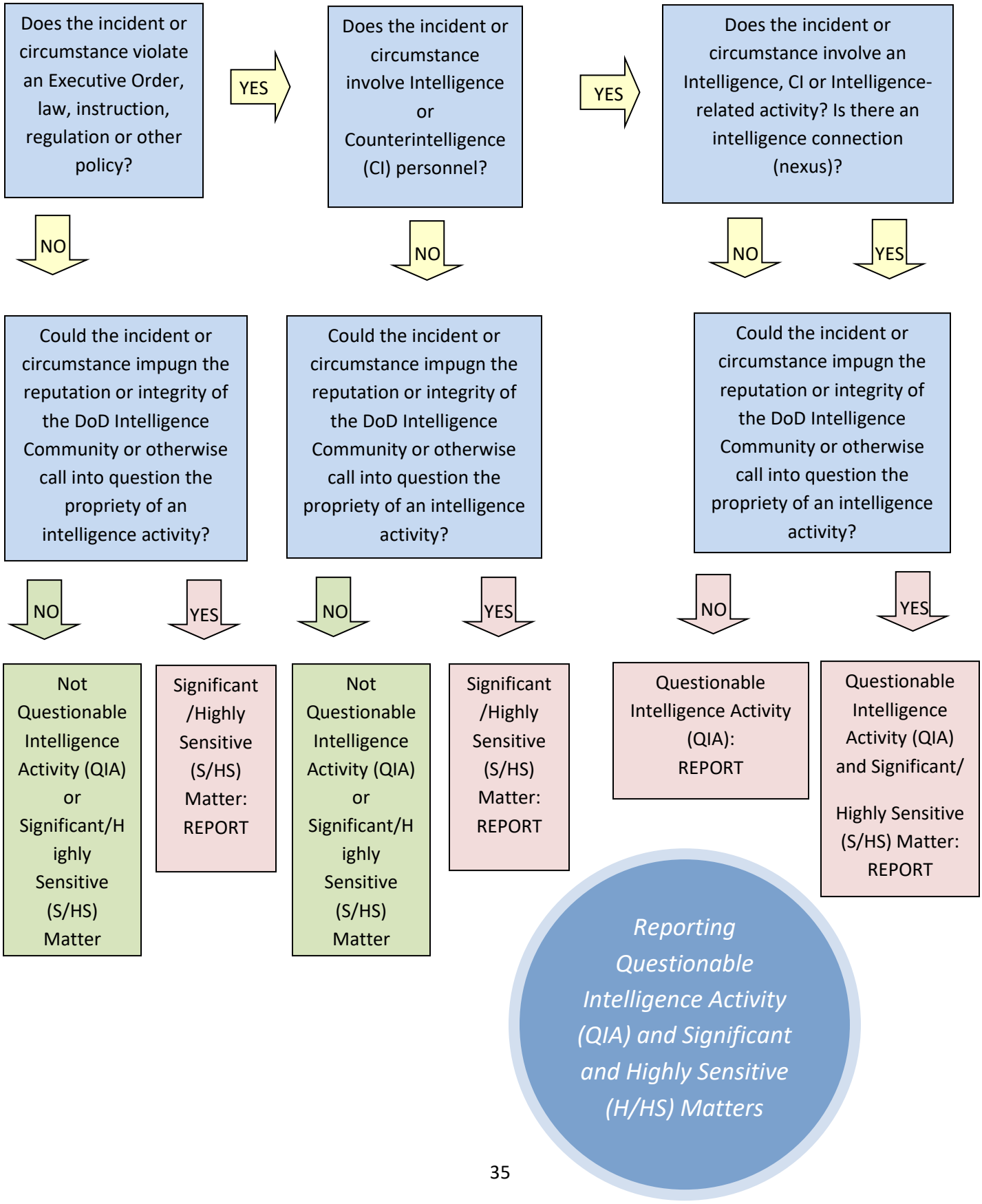
Click to open in PDF

1

KSARNG UNIT INTELLIGENCE OVERSIGHT CHECKLIST		
UNIT:	**DATE:**	
UNIT POC:	**INSPECTOR:**	
QUESTION	**SAT / UNSAT**	**REMARKS**
1. Is the Unit Commander, Director or SIO knowledgeable of the missions, plans, and capabilities of subordinate intelligence and intelligence-related units and does he/she levy tasks and missions IAW IO applicable law, policy and guidance? (CNGBI 2000.01, Enclosure A, Para. 14.b.)		
2. Has the Unit Commander, Director or SIO established and maintained an effective Intelligence Oversight program for all personnel assigned or attached to the organization? (CNGBI 2000.01, Enclosure A, Para. 14.c.)		
3. Has Unit Commander, Director or SIO appointed, in writing, experienced intelligence professionals to serve as primary and alternate IO Monitors? (CNGBI 2000.01, Enclosure A, Para 14.d.)		
4. Are copies of the IO Monitor appointment letter posted in the organization's workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01, Enclosure A, Para. 14.d.)		
5. Are all personnel able to identify the organization's IO Monitor and know how to establish contact? (CNGBI 2000.01, Enclosure A, Para. 16.f. and Para 15.b.)		
6. Does the Unit Commander, Director or SIO forward proposals for intelligence activities that may be questionable or contrary to policy to a Service JA and NG-JFHQs-State JA for review and submission to NGB-JA if required? (CNGBI 2000.01, Enclosure A. Para. 14.g.)		
7. Has the IO Monitor implemented an IO program that educates and trains intelligence personnel on applicable IO regulations and directives, as well as individual reporting responsibilities? (CNGBI 2000.01, Enclosure A, Para. 15.b.)		

KSARNG UNIT INTELLIGENCE OVERSIGHT CHECKLIST V2 (9JAN2018)

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



Annex L PUM Template

UNCLASSIFIED // FOR OFFICIAL USE ONLY

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
KANSAS ARMY NATIONAL GUARDJOINT FORCE HEADQUARTERS – KANSAS
2800 SOUTHWEST TOPEKA BLVD
TOPEKA, KANSAS 66611

NGKS-INZ xx August 2018

MEMORANDUM FOR NGB-J2

SUBJECT: Kansas National Guard (KSNG) Airborne Imagery Proper Use Memorandum (PUM) for RQ-11 Raven Small Unmanned Aircraft (SUAS) Title 32 Training, 01 January – 31 December 2019

1. (U/FOUO) References:

a. (U) Executive Order 12333, United States Intelligence Activities, 4 Dec 81, as amended

b. (U) DoD Directive 5148.13, Intelligence Oversight, 26 Apr 17

c. (U) DoD Manual 5240.01, Procedures Governing the Conduct of Intelligence Activities, 8 Aug 16

d. (U) DoD 5240.1-R, Change 2, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 26 Apr 17

e. (U) Deputy Secretary of Defense Policy Memorandum 15-002, Guidance for the Domestic Use of Unmanned Aircraft Systems, 17 Feb 15

f. (U) DoD Directive 3025.18, Defense Support of Civil Authorities (DSCA), 21 Sep 12

g. (U) Defense Intelligence Agency (DIA)/CL Message, New Procedures for the Approval of DoD Domestic Airborne Reconnaissance Imagery Proper Use Statements, DTG 282048Z Nov 01

h. (U) DIA/CL Message, Proper Use Statements for Domestic Imagery – Updated Guidance, DTG 231845Z Sep 96

i. (U) Army Regulation 381-10, U.S. Army Intelligence Activities, 3 May 07

j. (U) Department of the Army Memorandum, Implementing Guidance for Intelligence Oversight, 15 Aug 16

k. (U) Chief National Guard Bureau Instruction (CNGBI) 2000.01, National Guard Intelligence Activities, 04 Apr 17

l. (U) Chief National Guard Bureau Manual (CNGBM) 2000.01, National Guard Intelligence Activities, 26 Nov 12

m. (U) Chief National Guard Bureau Notice (CNGBN) 2000, Interim Revision to CNGB Series 2000.01, National Guard Intelligence Activities, 12 Oct 16

n. (U) CNGBI 7500.00, Domestic Use of National Guard Unmanned Aircraft Systems, 13 Oct 16

o. (U) KSNG 381-20 Intelligence Oversight, insert date

2. (U//FOUO) This PUM covers KSNG RQ-11 RAVEN SUAS Title 32 training missions flown by the 2-137th Combined Arms Battalion (CAB) within the local training area from 01 January through 31 December 2019. For the purposes of this PUM, the local training area is defined as Federal Aviation Administration (FAA) approved restricted airspace located at Fort Riley, KS. The purpose of these missions is to conduct realistic training and evaluation in core Federal military mission areas in order to maintain and increase the proficiency of UAS operators and maintainers. Named areas of interest are military targets, and may include tracking stationary and moving targets. Any tracking will only be conducted on government vehicles or approved vehicles in which the owner/operator has given consent to the unit to conduct the tracking exercise. The airborne platform and sensors to be used are the RQ-11 RAVEN SUAS with electro-optical/infrared (EO/IR) Full Motion Video (FMV). All platforms, sensor data and imagery products will be used for training and evaluation purposes to further enhance aircrew and ground crew proficiency KSNG UAS assets will NOT be employed for any purpose, such as Immediate Response or DSCA purposes, other than DoD-required training without specific Secretary of Defense approval IAW references e and f. All platforms, sensor data and imagery products will be used for training and evaluation purposes to further enhance aircrew and ground crew proficiency. Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and Measurement and Signatures Intelligence (MASINT) will **NOT** be collected or disseminated.

3. (U//FOUO) No U.S. persons will be targeted during these missions. Any personally identifying information unintentionally and incidentally collected about specific U.S. persons will be purged and destroyed unless it may be lawfully retained and disseminated to other governmental agencies that have a need for it IAW applicable laws, regulations, and policies.

4. (U//FOUO) Sensor data and imagery resulting from RQ-11 RAVEN SUAS collection efforts will be processed and exploited by 2-137th CAB aircraft operators, briefing officers, intelligence analysts and final flight approval officers. Raw imagery, analytic data, working copies and finished products will be used by participating personnel for training purposes only. Products will be will be disseminated in electronic formats in which the imagery/sensor data will be disseminated to users via a secure internal sharepoint. Some imagery and sensor data may be retained for training, planning or historical purposes; all other imagery and sensor data will be purged, deleted or destroyed at the end of each training mission. Any products retained will be reviewed at a minimum annually and destroyed or deleted when no longer required. All KSNG personnel involved in collecting, processing and exploiting, analyzing or disseminating imagery and products are subject to intelligence oversight (IO) and have received IO training.

5. (U//FOUO) “I certify that the intended collection and use of the requested information, materials, and imagery are in support of Congressionally approved programs and are not in violation of applicable laws. The request for imagery is not for the purpose of targeting any specific U.S. person (USPER), nor is it inconsistent with the Constitutional and other legal rights of U.S. persons. Applicable security regulations and guidelines, and other restrictions will be followed.” This PUM has been reviewed for legal sufficiency by MAJ Paul W.

Cope, Legal Advisor to the Adjutant General KSARNG, paul.w.cope2.mil@mail.mil at 785-646-1027 on _____.

6. (U//FOUO) CERTIFICATION: “I am authorized as a trusted agent and certifying official on behalf of the requesting unit, and I understand I am responsible for the accuracy of the information contained herein and for the proper safeguarding of products received in response.”

LTC Charles R. Harriman, SIO, 785-646-1327, charles.r.harriman.mil@mail.mil.

7. (U) Point of contact for this PUM is MAJ Daniel Jones at 785-646-0201 daniel.h.jones.mil@mail.mil

CHARLES R. HARRIMAN
LTC, MI, KSNG
Senior Intelligence Officer