CHIEF OF THE NATIONAL GUARD BUREAU MANUAL

NGB-J2 CNGBM 2000.01C
DISTRIBUTION: A 21 March 2025

THE CONDUCT AND OVERSIGHT OF NATIONAL GUARD INTELLIGENCE ACTIVITIES

References: See Enclosure K.

1. Purpose. This manual provides procedural guidance for the conduct and oversight of National Guard (NG) intelligence and intelligence-related activities in accordance with (IAW) reference a through reference g.

2. Cancellation. This manual cancels and replaces its previous edition, Chief of the National Guard Bureau (CNGB) Manual 2000.01B, 24 August 2022, "National Guard Intelligence Activities."

3. Applicability. This manual applies to the NG intelligence component, as defined in the glossary. This manual does not apply to criminal investigations or authorize any intelligence activity not otherwise permitted by law.

4. Procedures. Reference e establishes Attorney General-approved procedures to enable the Department of Defense (DoD) to conduct authorized intelligence activities in a manner that protects the privacy and civil liberties of U.S. persons.

a. Procedure 1 provides general guidance. Procedures 2, 3, and 4 articulate the exclusive procedures through which the NG intelligence component, IAW reference a, may collect, process, retain, and disseminate information concerning United States persons, hereinafter referred to as U.S. person information (USPI).

b. Procedures 5 through 10 define procedures regarding the use of special collection techniques to obtain information for foreign intelligence (FI) and counterintelligence (CI) purposes. Authority to employ these techniques is limited to that necessary to perform functions assigned to the DoD intelligence component concerned.

c. NG intelligence component will secure Secretary of Defense, Under Secretary of Defense for Intelligence and Security, or applicable Defense Intelligence Component Head approval to support law enforcement agencies and other civil authorities IAW reference d.

d. NG intelligence component personnel will follow Guidelines for Employees and conduct intelligence and intelligence-related activities only IAW reference a through reference g, this manual, and any other applicable regulations, instructions, policies, and procedures. Employees must ensure they have the appropriate mission and authority to conduct their activities, being careful not to exceed the authorities granted by law, Executive order, and applicable regulations and instructions. Employees of the NG intelligence component are trained IAW Enclosure E and will carry out reporting responsibilities as outlined in Enclosure C.

e. The NG intelligence component will comply with guidelines for identifying, reporting and investigating questionable intelligence activities (QIAs), significant or highly sensitive matters (S/HSMs), and Federal crimes committed by NG intelligence component personnel. The NG intelligence component is required to report misconduct incidents related to intelligence and intelligence-related activities that violate any Executive Order, law, policy, or regulation governing those activities, S/HSM, and Federal crimes to the NGB Inspector General (NGB-IG). Specific guidance is in Enclosure B.

f. Reference a and this manual does not authorize the conduct of intelligence, CI, or intelligence-related activities. An NG intelligence component element must have separate approved mission, authority, and purpose before conducting any intelligence or intelligence-related activity. While conducting authorized intelligence or intelligence-related activities, they will not exceed the authorities granted by law, Executive order, and applicable policy.

5. Summary of Changes. This manual has been revised to update the title, remove procedural guidance already contained in parent policy documents, and update the references. It reinforces that NG State Counterdrug Plan programs are conducting non-intelligence activity, are not subject to intelligence oversight, and are no longer required to receive intelligence oversight training. It expands the approval authority for proper use memorandums (PUMs) and domestic imagery legal reviews to include field grade warrant officers. It updates policy for intelligence support to law enforcement agencies and other civil authorities. It also states that the National Guard Bureau (NGB) Intelligence Oversight Monitor Certification Course is mandatory for all NG Intelligence Oversight (IO) monitors, and all NG Inspectors General (IGs) must complete IO training.

6. Releasability. This manual is approved for public release; distribution is unlimited. It is available at <https://www.ngbpmc.ng.mil/>.

7. Effective Date. This manual is effective upon publication and must be reviewed annually by the Proponent/Office of Primary Responsibility for continued validity, and must be revised, reissued, cancelled, or certified as current every ten years.

DARRIN E. SLATEN
Major General, USAF
National Guard Bureau Director of Staff

Enclosures:

A -- Procedures
B -- Identifying, Investigating, and Reporting Questionable Intelligence Activity, Significant or Highly Sensitive Matters, and Reportable Federal Crimes
C -- Intelligence Oversight Training Requirements
D -- Domestic Operations
E -- Domestic Imagery
F -- Intelligence Support to Force Protection
G -- The Internet and Publicly Available Information
H -- Intelligence Oversight Continuity Binder
I -- Compliance Inspection Guidance and Self-Inspection Checklists
J -- Intelligence Oversight Process
K -- References
GL -- Glossary

ENCLOSURE A

PROCEDURES

1. Procedure 1: General Provisions.

a. All NG personnel will conduct intelligence and intelligence-related activities pursuant to reference b and only IAW reference a, reference c through reference g, and this manual; personnel will not exceed the authorities granted by these references or applicable laws, Executive orders, regulations, instructions, or policies. For the DoD, authorized intelligence activities are defense-related FI and CI conducted pursuant to reference b. The NG in a status provided under Title 32 United States Code (T32 status) status trains to perform these missions. Intelligence activity conducted in T32 status requires authorization by the Secretary of Defense (SecDef) or their designee. In all circumstances, intelligence and intelligence-related activities will be carried out IAW reference h and the laws of the United States (U.S.).

b. NG intelligence component elements may not investigate U.S. persons (USPERs) or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment to reference h or the lawful exercise of other rights secured by reference h and laws of the U.S. NG intelligence component elements are not authorized to, and will not engage in, any intelligence activity for the purpose of affecting the U.S. political process, including dissemination of information to the White House. NG intelligence component elements will not participate in or request any person or entity undertake any activities that are forbidden by reference b and reference d.

(1) Example. Prior to elections, peaceful protests are taking place across the U.S. A senior leader tasks T32 NG intelligence personnel with researching and reporting on the most active protest groups. May Intelligence personnel do this? No, it is outside the scope of their mission and authority. NG intelligence personnel may advise the senior leader to consult with the Provost Marshal or law enforcement branch IAW paragraph 1.b of this section and reference e.

(2) Example. The protests have devolved into violent civil unrest. A senior military leader tasks intelligence personnel in T32 status with researching and reporting on groups and their activities. May intelligence personnel provide support? No, this is still outside the scope of their mission and authority IAW paragraph 1.a of this section and reference e. NG intelligence personnel may advise the senior leader to consult with the Provost Marshal or law enforcement branch.

2. Procedure 2: U.S. Person Information (USPI) Collection. This procedure specifies the general criteria governing USPI collection. NG Intelligence component personnel must have explicit mission and authority to conduct intelligence collection. Any authorization for T32 NG intelligence activity will define the authorized collection and designate the Defense Intelligence Component Head responsible for guiding and overseeing the activity.

3. Procedure 3: USPI Retention.

a. Intelligence component elements will evaluate all information that may contain USPI within the established timelines (see Table 1) to determine whether it meets the permanent retention standard of reference e and may be permanently retained.

Type of Collection	Location of U.S. Person	Evaluation Period for Retention Determination	Extension
Intentionally collected USPI	Inside or outside the U.S.	Promptly, or up to 5 years if necessary	5 years Approved by Defense Intelligence Component Head May be given at time of collection or later
Incidentally collected USPI	Inside the U.S.	5 years	5 years Approved by Defense Intelligence Component Head May be given at time of collection or later
Incidentally collected USPI	Outside the U.S.	25 years	No extension
Voluntarily provided USPI	Inside or outside the U.S.	Promptly, or up to 5 years if necessary	5 years Approved by Defense Intelligence Component Head May be given at time of collection or later
Special circumstances	Inside or outside the U.S.	5 years	5 years Approved by the Undersecretary of Defense for Intelligence and Security. May be given at time of collection or later
Disseminated by another DoD intelligence component or Intelligence Community elements	Inside or outside the U.S.	Same time as originating entity	No extension

Table 1. Evaluation Periods for Permanent Retention of USPI

b. If the USPI meets the permanent retention standard, NG intelligence component elements will maintain an internal memorandum for record (MFR) that documents the reason for permanently retaining the USPI and the authority approving the retention. A template is contained in Figure 1.

1. DESCRIPTION OF USPI RETAINED	
2. DATE COLLECTED	
3. Type of collection (circle one)	• Intentional • Incidental • Voluntarily provided • Special circumstance • Disseminated by another DoD Intelligence Component or Intelligence Community element
4. IF DISSEMINATED BY ANOTHER DOD INTELLIGENCE COMPONENT OR INTELLIGENCE COMMUNITY ELEMENT, WHICH ONE?	
5. LOCATION OF U.S. PERSON(S) WHEN COLLECTED	
6. AUTHORIZED MISSION SUPPORTED	
7. WHY IT IS REASONABLY BELIEVED TO BE NECESSARY TO PERMANENTLY RETAIN THE USPI	
8. APPROVED CATEGORY(IES) OF INFORMATION UNDER WHICH THE USPI FALLS (CIRCLE ALL THAT APPLY)	• Publicly available information • Information obtained with consent • Information reasonably believed to constitute Foreign Intelligence • Counterintelligence • Threats to safety • Protection of intelligence sources and methods • Current, former, or potential sources of assistance to intelligence activities • Persons in contact with sources of potential sources • Physical security • Personnel security • Communications security (COMSEC) investigation • Overhead and airborne reconnaissance (not for targeting specific U.S. persons) • Administrative purposes
9. MEANS OF COLLECTION	

I have approved the justification for permanent retention and reasonably believe it is necessary for an authorized mission, falls within an approved category of information, and was properly collected.

[J2, G2, A2, Senior Intelligence Officer, or Commander signature block]

Figure 1. Documenting Decisions to Permanently Retain USPI

c. Marking Electronic and Paper Files.

(1) In accordance with reference e, intelligence files and documents that contain USPI, whether retained in print, electronic format, or posted to an Internet website, must contain a USPER warning notice like the one in Figure 2.

"ATTENTION: This document contains U.S. person information (USPI), which has been included consistent with all applicable laws, directives, and policies. The information has been deemed necessary for the intended recipient to understand, assess, or act on the information. It must be handled in accordance with the recipient's intelligence oversight or information protection and handling procedures."

Figure 2. USPI Warning Notice

(2) This requirement applies regardless of whether the USPER is the subject of intentional or incidental collection. In the case of electronic files, if it is not reasonably possible to mark individual files containing USPI, this requirement may be satisfied with an access banner identifying that users may encounter USPI. Individual intelligence products must be marked appropriately. Any USPER source reference citations, such as The Washington Post, must also be marked as USPER (in other words, "(USPER) The Washington Post"). Intelligence component personnel must determine whether it is appropriate for intelligence products posted for general access to contain specific USPI. If the determination is made to minimize or redact such information, then the product posted should clearly indicate how that USPI may be obtained should a mission require it. A sample notice is contained in Figure 3.

"Other U.S. person information has been minimized. Should you require the minimized U.S. person information, please contact [insert spelled out office (office symbol) and telephone number]."

Figure 3. Notice Regarding Minimized USPI

(3) The warning notice is not required if the document or file includes only a reference to an unnamed or unidentified USPER.

(4) The first time a USPER appears in a document, the marking "USPER" will precede the name or alias. This designator must be used only the first time the name of the USPER appears in the product.

d. Annual File Reviews. NG intelligence component elements will review all electronic and hardcopy files at least once every calendar year to ensure that USPI retention is still necessary for an authorized function, has not been held beyond established disposition criteria, and is not retained in violation of the established permanent retention standard. They will also review information systems containing USPI and audit queries or other search terms to assess compliance with this issuance. Intelligence oversight monitors will maintain an internal MFR on file in the Intelligence

Oversight (IO) Continuity Binder to certify that the review was conducted, that no unauthorized USPI has been retained and no unlawful or improper queries of USPI have been made or will be maintained. See Figure 4 for a sample template.

[Day Month Year]

MEMORANDUM FOR RECORD

Subject: Annual File Review

Reference: Chief of the National Guard Bureau Manual 2000.01D, [Date], "The Conduct and Oversight of National Guard Intelligence Activities"

1. I certify that, in accordance with Enclosure A, paragraph 3.d. of the reference, the [UNIT/STAFF] has reviewed all electronic and hardcopy files, and no unauthorized U.S. person information is being retained or held beyond established disposition criteria.

2. Point of contact is [NAME]; [TELEPHONE].

[FIRST AND LAST NAME]
[Rank, USA/USAF]
[Commander/Director/SIO]

Figure 4. Annual File Review Certification Template

4. Procedure 4.

a. USPI Dissemination. The NG intelligence component may disseminate USPI information only IAW reference e. Table 2 shows USPI dissemination categories with criteria and additional rules.

Category	Criteria	Additional Rules
Any person or entity	Information is publicly available, or the information concerns a U.S. person who has consented to the dissemination.	None
Other Intelligence Community elements	Dissemination is for the purpose of allowing the recipient to determine whether the information is relevant to its responsibilities and can be retained.	None
Other DoD elements	The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.	None
Other Federal Government entities	The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.	The Defense Intelligence Component Head must approve any dissemination that is not for FI, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes.
State, local, Tribal, or Territorial governments	The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.	The Defense Intelligence Component Head must approve any dissemination that is not for FI, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes.

Table 2. USPI Dissemination Categories with Criteria and Additional Rules

Category	Criteria	Additional Rules
Foreign governments or international organizations	The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions, and the Defense Intelligence Component head or a delegee has determined that the disclosure is consistent with applicable international agreements and foreign disclosure policy and directives, including those policies and directives requiring protection against the misuse or unauthorized dissemination of information, and the analysis of potential harm to any individual.	The Defense Intelligence Component Head must approve any dissemination that is not for FI, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes.
Assistance to the component	Dissemination is to a Governmental agency, an international entity, or an individual or entity not part of a government and is necessary for the limited purpose of assistance to the NG.	The disseminator will inform the recipient that it should do all the following, except in exceptional circumstances where providing such information is inconsistent with operational requirements, as determined by the Defense Intelligence Component Head: (1) Use the information only for this limited purpose. (2) Properly safeguard the information. (3) Return or destroy the information when it has provided the requested assistance. (4) Not disseminate the information further without the prior approval of the Defense Intelligence Component.

Table 2, continued. USPI Dissemination Categories with Criteria and Additional Rules

Category	Criteria	Additional Rules
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.	For any dissemination of USPI to individuals or entities not part of a government, the Defense Intelligence Component Head will assess the risk associated with such dissemination, consider whether any further restrictions or handling caveats are needed to protect the information, and comply with any limitations required by foreign disclosure policy.
Required disseminations	Dissemination is required by statute; treaty; Executive order; Presidential directive; National Security Council guidance; policy, memorandum of understanding, or memorandum of agreement approved by the Attorney General; or by court order.	None

Table 2, continued. USPI Dissemination Categories with Criteria and Additional Rules

b. Improper USPI Dissemination. Any improper dissemination or suspected improper dissemination of USPI will be reported as a QIA immediately upon discovery IAW Enclosure B and reference i.

5. Procedure 5: Electronic Surveillance.

a. Governing Principles. Section 1 of reference j lays out the governing principles for signals intelligence (SIGINT) collection. The National Security Agency (NSA) is the only organization that authorizes SIGINT collection activities. Under no circumstances may units perform SIGINT collection activities independently or under the direction of a Governor in support of a State mission. SIGINT is heavily regulated because it involves electronic surveillance, a very intrusive activity covered by the Fourth Amendment to reference h. Units conducting SIGINT will be familiar and comply with applicable NSA Central Security Service United States Signals Intelligence Directives (USSIDs) included in reference k through reference q.

b. Mission and Authority. NG intelligence component elements with mission and authority may only conduct electronic surveillance under Title 10 (T10) authority. No mission involving SIGINT or electronic surveillance may be independently initiated using T32 authorities but may be staffed with NG personnel on T32 orders if properly assigned to that mission. Commands that have SIGINT cryptologic elements will ensure that those elements conduct activities IAW applicable USSIDs, such as

reference k through reference q. USSIDs are an extensive set of NSA directives that define controls and operating procedures for SIGINT activities and possess the same regulatory power over SIGINT operations as an Army Regulation or Air Force Instruction. USSIDs require separate IO programs and reporting requirements for NG personnel conducting SIGINT.

c. Army National Guard (ARNG) SIGINT Production Chain. The ARNG SIGINT IO program is managed solely within the Army SIGINT Production Chain. This ensures that incidents involving the compromise of SIGINT information remain within the Army SIGINT Production Chain under the purview of the NSA. Reference l explains the detailed requirements of the Army SIGINT Oversight Program and defines the roles and responsibilities of the various positions involved in the process. IAW reference l, ARNG SIGINT elements that conduct SIGINT activities or training exercises during the reporting period must submit a Quarterly IO Report and Commander's Signature page. If submitting early, units must annotate that "no SIGINT will be conducted for the remaining days of the quarter" in the Additional Information section at the end of the report. Submit all reports using email to the Guard Technical Control and Analysis Element at <usarmy.meade.inscom.list.gtcae@army.mil>.

d. Technical Surveillance Countermeasures (TSCM). This section applies to the NGB Joint Intelligence Directorate (NGB-J2) TSCM team, which uses specialized electronic equipment and techniques to support the CNGB by detecting the existence and capability of electronic surveillance equipment being used for unauthorized electronic surveillance. IAW approval granted by the Undersecretary of Defense for Intelligence and Security in reference r, the NGB-J2 TSCM team may conduct their activity only IAW reference e and reference s.

6. Procedures 6 through 10:

a. NG FI and CI elements in a T32 status are not authorized to conduct concealed monitoring (Procedure 6), physical searches (Procedure 7), searches of mail and use of mail covers (Procedure 8), physical surveillance (Procedure 9), and undisclosed participation in organizations (Procedure 10) in the U.S. IAW reference b, these restrictions do not apply when activities are conducted as part of testing or training when the subjects are participants and have fully consented to the activity as part of an approved testing or training plan.

b. Procedure 10: Undisclosed Participation in Organizations. NG intelligence component employees do not require permission to participate in organizations for the following purposes:

(1) Education or training. Attending a course, meeting, seminar, conference exhibition, trade fair, workshop, or symposium, or participating in educational or professional organizations for the sole purpose of obtaining training or enhancing professional skills, knowledge, or capabilities. Directing or tasking employees to conduct intelligence activities is not authorized.

(2) Personal purposes.

7. Assistance to Law Enforcement Agencies and Other Civil Authorities. This provision applies to NG intelligence component support to any Federal, State, Territorial, Tribal, or local civilian law enforcement agency or other civil authority.

a. Requests for NG intelligence support to civilian law enforcement agencies and other civil authorities. These requests are closely reviewed and processed separately for approval. Refer to Table 3 and reference d for approval authority for this support.

Activity	Purpose	Authority	Approval
Intelligence activity	FI or CI support.	Operating under Federal Intelligence authorities, such as providing counterdrug (CD) Federal intelligence support to a law enforcement authority under the authority of reference t.	SecDef or delegee approval required.
Intelligence-related activity	Training on intelligence mission-essential task lists or tradecraft (as the primary purpose of the activity) to meet informational requirements of or to otherwise support a law enforcement authority (as an incidental or secondary purpose).	Operating under T32 training authorities for the primary purpose of intelligence training.	SecDef or delegee approval required.

Table 3. Approval Authority for LEA Support

(1) Intelligence Activities. When the request for support to a civilian law enforcement agency or other civil authority involves the provision of FI or CI support, it is considered an intelligence activity subject to IO and will be processed for SecDef or delegee approval IAW reference d.

(2) Intelligence-Related Activities. When the request for support to a civilian law enforcement agency or other civil authority involves leveraging intelligence training to provide an incidental benefit to law enforcement, it is considered an intelligence-related activity also subject to IO and will be processed for SecDef or delegee approval IAW reference d.

(3) Use of Federal Intelligence and Intelligence, Surveillance, and Reconnaissance (ISR) Equipment. When the request for support to a civilian law enforcement agency or other civil authority involves the use of Federal intelligence or ISR equipment, it will be processed for SecDef approval IAW reference d.

b. NG intelligence component elements may provide incidentally acquired information reasonably believed to indicate a violation of law to the appropriate law enforcement agency through the NGB Antiterrorism and Critical Infrastructure Protection Branch (NGB-J34), force protection (FP), or law enforcement channels and must protect any applicable sensitive sources and methods. Dissemination of any USPI will be conducted IAW Procedure 4 reference e.

c. See Enclosure D, paragraph 4, for specific CD guidance.

d. Requests for assistance from federal law enforcement agencies or other civil authorities requiring SecDef approval under this procedure will be routed from the federal law enforcement agency to the DoD. Requests for support to local, state, tribal, or territorial law enforcement agencies requiring SecDef or delegee approval under reference d will be staffed from the Director of NG Joint Force Headquarters–State (NG JFHQs-State) J2 to NGB-J2. The following documents are required: a request for assistance from the law enforcement authority, a request for SecDef approval from The Adjutant General (TAG) or the Commanding General of the District of Columbia (CG), a legal review by the State Judge Advocate (JA) validating the legality of providing NG intelligence component support, a concept of operations for the support, and a memorandum of agreement between the NG JFHQs-State and the supported law enforcement authority. An electronic template is available for download on the NGB-J2-IO Section website found in reference u.

ENCLOSURE B

IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE INTELLIGENCE ACTIVITY, SIGNIFICANT OR HIGHLY SENSITIVE MATTERS, AND REPORTABLE FEDERAL CRIMES

1. Reporting. IAW reference c, NG intelligence staffs, units, and personnel must report QIA and S/HSM to their IG immediately upon discovery through their chain of command or supervision IAW procedures identified in reference i. Immediately upon discovery, they must also report to their JA or IG, through their chain of command or supervision, the facts or circumstances that reasonably indicate that an NG intelligence component employee has committed, is committing, or will commit a violation of Federal criminal law. If it is not practical to report to the chain of command or supervision, reports may be made through NG JFHQs-State J2; JA or IG, or NGB-J2; NGB Office of the General Counsel (NGB-GC); or NGB Inspector General channels by procedures identified in reference i.

a. QIA. IAW reference c, QIA is any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive order, Presidential directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

b. S/HSM. IAW reference c, an S/HSM is an intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an Executive order, Presidential directive, Intelligence Community directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential:

(1) Congressional inquiries or investigations.

(2) Adverse media coverage.

(3) Impact on foreign relations or foreign partners.

(4) Systemic compromise, loss, or unauthorized disclosure of protected information. (This does not include reporting routine security violations.)

2. Identifying QIA. An activity is not a QIA unless some connection exists between the activity and an intelligence function; only those QIAs occurring as part of intelligence or intelligence-related duties, or missions will be reported. Illegal or improper activities performed by intelligence or intelligence-related personnel in their personal capacity which have no relationship to the intelligence mission (for example, breach of discipline and simple security or ethics violations) are not subject to QIA reporting and will be handled through normal disciplinary or law enforcement channels.

3. Examples of QIA. The following are examples of commonly reported QIA:

a. Improper USPI collection, retention, or dissemination. This includes:

(1) Gathering information about U.S. domestic groups not connected with a foreign power or international terrorism.

(2) Producing and disseminating intelligence threat assessments containing USPI without a clear explanation of the intelligence purpose for which the information was collected.

(3) Incorporating criminal information on a USPER into an intelligence product without determining whether identifying the person is appropriate.

(4) Collecting USPI for FP purposes without determining whether the intelligence function related to it is authorized (for example, collecting information on the domestic activities of U.S. persons).

(5) Collecting publicly available USPI without a logical connection to the unit intelligence mission.

(6) Disseminating FP information on USPERs and their domestic activity as an intelligence product (for example, including USPERs groups in an intelligence annex as enemy forces).

b. Failure to file a PUM for airborne domestic imagery collection.

c. Tasking intelligence personnel to conduct intelligence activities that are not part of the organization's approved mission, even if they have the technical capability to do so.

d. Misrepresentation, which includes the following:

(1) Using the status of a Military Intelligence Soldier or Airman to gain access for non-intelligence purposes (for example, an intelligence traditional Guardsman accessing DoD intelligence databases to gain information for a civilian job).

(2) Claiming to be conducting a highly classified activity or an investigation for personal gain, for unauthorized access, or to impress or intimidate anyone.

e. QIA constituting a crime, which includes the following:

(1) Stealing a source payment during a deployment.

(2) Using intelligence funds for personal gain.

(3) Falsifying intelligence or investigative reports.

(4) Stealing private property while searching for exploitable documents and materiel during a deployment.

(5) Stealing or allowing another to steal private property while using non–U.S. government facilities for intelligence purposes.

f. Searching or monitoring private Internet accounts of a USPER under the guise of determining whether the individual was passing classified information without an authorized CI or law enforcement investigation and proper search or electronic surveillance authority.

g. Creating a fake social media account to monitor the activity of a USPER without mission and authority.

h. Misconduct in the performance of intelligence duties, which includes the following:

(1) Falsifying investigative reports or personnel security investigation interviews.

(2) Coaching a source or subject of an investigation before an intelligence polygraph examination to help the individual pass the polygraph.

(3) Alleged abuse and mistreatment of detainees and prisoners by or directed by intelligence personnel during a deployment.

4. Reports Not Meeting QIA Criteria. The following are some examples of reports that do not meet QIA reporting criteria, unless there is a direct connection to an intelligence activity:

a. Security violations not directly connected to an intelligence activity, such as negligence in handling or storing classified information.

b. Not following instructions or policy and other similar acts of personal misconduct more appropriately dealt with through normal command actions, unless occurring while conducting an intelligence activity or otherwise meeting Federal crimes reporting criteria.

c. Being absent without leave or having special category absences.

d. Driving while intoxicated or driving under the influence.

e. Drug use or sale.

f. Suicide or attempted suicide.

5. Reporting CI Activities, Criminal Violations, and Federal Crimes.

a. Intelligence personnel also have an obligation to report significant CI activities, criminal violations, instances of espionage, and other possible Federal crimes IAW

reference b, reference c, reference v, and reference w. This ensures that senior DoD and Department of Justice leadership are aware of serious Federal crimes involving NG intelligence personnel and possible violations of Federal law by others that may come to the attention of intelligence personnel. This report does not replace existing investigative, judicial, or command authority and reporting requirements.

(1) Significant CI activities that involve significant matters or are likely to receive publicity.

(2) Criminal violations that must be reported are those involving:

(a) Allegations of fraud or theft when the subject is an installation commander or in or retired from the military grade of Colonel (O-6) and above or civilian General Schedule or General Grade 15 and above, and the potential loss to the Government is $5,000 or more.

(b) Any criminal corruption related to procurement involving current or retired DoD military or civilian personnel.

(3) Espionage is the act of securing information of a military or political nature that a competing nation holds secret. It can involve the analysis of diplomatic reports, publications, statistics, and broadcasts, as well as spying, or a clandestine activity carried out by an individual or individuals working under a secret identity to gather classified information on behalf of another entity or nation.

b. Reports of Federal crimes involving T32 NG intelligence personnel will be made through command channels to the NGB-J2 no later than five working days after discovery or receipt. The following will be included in the report:

(1) The fullest possible identification of the person committing the alleged Federal crime such as name, rank or civilian grade, Social Security number, military or civilian occupational specialty code, security clearance and current access, unit of assignment, employment, attachment or detail, and duties at the time of the alleged criminal activity. When the suspect's identity is unknown, as much detail as possible will be provided about the alleged crime. Clearly state that the suspect has not yet been identified and name the agency investigating. "John Doe" or other false names will not be used to refer to suspects. An additional report will be submitted when the suspect is identified.

(2) When and where the alleged crime occurred.

(3) A description of the Federal law that may have been violated.

(4) Identity of the law enforcement agency receiving the report and investigating the incident.

(5) If the report originated outside the affected command, whether the command submitted its own report and, if so, through what channels (for example, IO channels).

c. NGB-J2 will transmit reports received to the Office of the DoD Senior Intelligence Oversight Official.

d. Examples of reportable Federal crimes include espionage, sabotage, unauthorized disclosure of classified information, conspiracy to overthrow the U.S. Government, crimes involving foreign interference with the integrity of U.S. Government institutions or processes, crimes involving intentional infliction of serious physical harm or threat of death, unauthorized transfer of controlled technology to a commercial or foreign entity, and tampering with, or gaining unauthorized access to, information systems.

e. The following are examples of some non-reportable Federal crimes:

(1) Crimes committed by non-intelligence employees who are under investigation by a criminal investigative organization.

(2) Crimes against property totaling $500 or less for intelligence employees.

(3) Except for homicide or espionage, crimes committed more than 10 years before the NG intelligence element became aware of them. If, however, the intelligence component reasonably believes the criminal activities were or are part of a pattern of criminal activities, then they are reportable no matter when the activity occurred.

ENCLOSURE C

INTELLIGENCE OVERSIGHT TRAINING REQUIREMENTS

1. Training Requirements.

a. The following personnel must receive IO training:

(1) All NGB, T32 NG JFHQs-State, and T32 NG intelligence staffs, organizations, and units, as well as T32 non-intelligence organizations that perform intelligence or intelligence-related activities, as defined in the glossary, also known as the NG intelligence component.

(2) All NGB and T32 service members, civilian, and contractor personnel assigned or attached to the units and staffs listed in paragraph (1) above on a permanent or temporary basis, regardless of military specialty or job function.

(3) Contractors or consultants assigned or attached to the units and staffs listed in paragraph (1) above who are conducting intelligence or intelligence-related activities or supporting intelligence efforts.

(4) In accordance with reference x, all T32 ANG units and staffs that conduct information operations.

(5) In accordance with reference y, all T32 ANG Operations Security Program Managers, Signature Managers, Planners, and AF Operations Security Support Team members.

(6) TAGs, CG, Commanders, and directors responsible for the personnel listed in paragraph (1).

(7) JAs or GCs of those organizations who conduct or provide legal advice regarding intelligence or intelligence-related activities.

(8) All NG IGs.

b. IO training will consist of initial, annual refresher, and, if applicable, pre-deployment training.

(1) Initial Training. IO Monitors will provide initial IO training to all personnel within 90 days of assignment or employment.

(2) Annual Refresher Training. IO Monitors will provide all personnel refresher IO training annually. For example, if you received IO training on 24 January of this year, you are required to receive IO training no later than 24 January the following year.

(3) Pre-Deployment or Temporary Duty Training. IO Monitors will ensure that training for all personnel deploying to another duty location remain current for the

duration of the deployment or temporary duty. If training is scheduled to lapse during the deployment or temporary duty, then refresher training will be provided before departure; this training will fulfill the annual refresher training requirement.

c. Intelligence Oversight Monitors are required to complete the NGB Intelligence Oversight Monitor Certification Course available on milSuite milUniversity at reference z as their initial and annual IO training and will maintain the certificate of course completion in the IO Continuity Binder.

2. Training Records. Organizations will maintain records of initial and annual training. All IO training records will be maintained for a minimum of three calendar years. Training records may be maintained in hard copy or electronic form and will be readily accessible.

3. Training Development.

a. Training is tailored to the staff, unit, or organization mission and will cover, at a minimum, the following:

(1) Purpose of the IO Program.

(2) Applicability (to whom IO applies) and how duty status (T10, T32, or State Active Duty) affect applicability.

(3) Authorized Federal and State mission(s) of the staff, unit, or organization.

(4) Familiarity with the authorities and restrictions established in NGB, Service, and DoD policies applicable to authorized intelligence and intelligence-related activities.

(5) Standards of employee conduct.

(6) Procedures 1 through 4.

(7) Any other procedures that apply to the staff, unit, or organization. For example, units with a SIGINT mission must be trained in Procedure 5. Units with CI or Human Intelligence (HUMINT) missions must be trained in Procedures 6 through 10. Units with an Open Source Intelligence mission must be trained on Procedure 10.

(8) Staffs, units, or organizations that collect, process, exploit, analyze, disseminate, or retain domestic imagery, or conduct incident awareness and assessment (IAA) will be trained on domestic imagery policy, including requirements for internal MFRs, PUMs, and Domestic Imagery Legal Reviews (DILRs).

(9) Responsibilities and procedures for identifying, reporting, and investigating QIA, S/HSM, and Federal crimes.

(10) Quarterly IO reporting.

(11) Applicable special focus areas, such as the use of the intelligence component for NG domestic operations (DOMOPS) missions, intelligence support to FP, use of the Internet, and use of publicly available information, including social media, applicable to the staff, unit, or organization.

(12) Civil liberties and privacy protections that apply to USPI.

b. To develop tailored training, units may download data from the folders on the NGB-J2 IO Guard Knowledge Online website (see reference aa). The DoD Senior Intelligence Oversight Official provides IO training resources to assist in developing unit-specific IO training at reference aa.

4. Additional Training Requirements for SIGINT Units. Commands with SIGINT elements will ensure that those elements obtain appropriate training from qualified personnel on applicable SIGINT directives. Reference e also requires training on the requirements and restrictions of reference t and reference b with respect to the unauthorized acquisition and use of communications and information. Reference l delineates policies and procedures to ensure that the missions and functions of the U.S. SIGINT System are conducted in a manner that safeguards the Constitutional rights of U.S. persons. All U.S. SIGINT System personnel who collect, process, retain, or disseminate SIGINT information must read reference j through reference q and be familiar with their contents. All NG commands that have SIGINT cryptologic elements must also be aware of NSA reporting requirements for SIGINT, as routine, U.S. garrison-based IO reporting responsibilities vary greatly from reporting requirements while in T10 status.

ENCLOSURE D

DOMESTIC OPERATIONS

1. Homeland Defense. Certain NG units support homeland defense missions, including aerospace control alert, air defense, defense critical infrastructure protection, and anti-missile defense. Mission and authority for NG intelligence activities include conducting these homeland defense missions as well as planning, preparing, and training for them. All collection, retention, and dissemination of information will be carried out IAW Procedures 2 through 4 of this manual and reference e.

2. Homeland Security. NG intelligence component personnel with the mission and authority may collect, analyze, and disseminate information IAW Procedures 2 through 4 of this manual and reference e. If asked to support homeland security intelligence activities, all NG assets must be aware of their authority, status, funding, and intent. The determination of compliance with intelligence oversight guidance can be complex; when in doubt, seek unit or State JA or NGB-GC guidance, and consider the following questions:

a. Is there a foreign connection?

b. Is it part of the element's mission-essential task list?

c. Is it within the purpose of the funding being used?

d. Are the activities overt and transparent?

e. Has any USPI been properly safeguarded and have rights to privacy been protected?

3. NG Domestic Support. When authorized upon receipt of an NG JFHQs-State or NGB--validated primary agency or lead Federal agency request for assistance, NG intelligence component personnel may fulfill TAG and CG requirements for situational awareness or planning purposes with non-intelligence equipment. Federal intelligence or Federal ISR equipment may be used only when approved by the SecDef, the SecDef's delegee, or an appropriate approval authority, or as directed by the President.

a. Search and Rescue (SAR). Upon a State, Tribal, Territorial, or local request, or a request by the appropriate Rescue Coordination Center, the T32 NG may provide support for SAR missions with non-intelligence equipment. Use of Federal ISR equipment for SAR requires prior approval of the SecDef for manned ISR platforms or the Commanders of U.S. Northern Command or U.S. Indo-Pacific Command for unmanned aircraft systems or remotely piloted aircraft. USPI may be collected during SAR missions; if a person is at risk of death or injury, consent is implied. However, once the SAR mission is completed, all USPI will be purged. Standing SAR DILRs are filed annually for use of non-intelligence equipment for SAR. Each approved use of Federal ISR, Remotely Piloted Aircraft (RPA), or Unmanned Aircraft System (UAS) equipment for SAR requires a separate PUM or DILR.

b. IAA. NG intelligence component personnel and non-intelligence equipment may be used for IAA to fulfill TAG or CG requirements for situational awareness or planning purposes, or upon receipt of an NG JFHQs-State, NGB-validated primary agency, or NGB-validated lead Federal agency request for assistance. IAA activities will not be used to collect USPI without consent. The agency must be operating within its lawful function and authority, such as at the request of the office of the Governor; the primary or lead Federal, State, Territorial, or Tribal agency for the event; a mutual aid or assistance agreement (for example, an Emergency Management Assistance Compact request); or a Mission Assignment from the Federal Emergency Management Agency or other lead Federal agency.

(1) When authorized by the SecDef or delegee, or as directed by the President, NG intelligence capabilities may support Federal, State, Territorial, Tribal, and local agencies in certain IAA mission sets, including situational awareness; SAR; damage assessment; evacuation monitoring; chemical, biological, radiological, nuclear, and high-yield explosives assessment; hydrographic survey; and dynamic ground coordination.

(2) During DOMOPS, the NG T32 intelligence component may use unclassified equipment to process, assess, and disseminate final products based on the analysis of:

(a) Imagery, geospatial data, and information collected from cameras, video, electro-optical sensors, infrared, and forward-looking infrared radar collected by NG assets.

(b) Information collected from Government agencies operating within their lawful functions and authorities.

(c) Analysis of baseline imagery for operational planning (for example, to determine probable hurricane landfall and post-landfall damage and to assess damage).

(3) Upon SecDef approval, the NG T32 intelligence component may use Federal intelligence equipment to process, assess, and disseminate final products within the parameters set by the SecDef.

(4) National Guardsmen may use only approved official Federal Government equipment for authorized collection. Under no circumstances are National Guardsmen permitted to use personal equipment, such as cameras, action cameras, personal cellphone cameras, or drones, for official purposes.

4. Counterdrug (CD) Support.

a. Drug Interdiction and CD Activities–State Plan Support.

(1) The primary purpose of all activity conducted for State CD plan support must be “drug interdiction and counterdrug activities.” IAW reference bb, drug interdiction and CD activities with respect to the T32 NG mean “the use of NG personnel in drug interdiction and CD law enforcement activities, including drug demand reduction

activities, authorized by the law of the State and requested by the Governor of the State."

(2) Intelligence and intelligence-related activity is not authorized under reference bb for State CD plan support. IAW reference cc, Service members on State Plans support are conducting a non-intelligence activity and as emphasized in reference bb, are subject to reference dd and reference ee. Protection of non-DoD affiliated person (NDAP) information policy training will be included in doctrinal training given to each member at initial entry and repeated annually for all personnel. See reference ff and reference gg for additional information.

(3) NG personnel providing criminal analysis support to civilian law enforcement agencies, a non-intelligence activity, under the authorities of reference aa and the approved State CD plan, will comply with reference cc and reference ee. IAW reference cc, analysts will follow the Federal, State, and local laws for handling criminal evidence and the supported agency's information handling policies and procedures to ensure compliance with applicable privacy laws and protect the rights of U.S. persons. Law enforcement criminal information will not be processed or stored on DoD systems.

(4) Any use of Federal intelligence, ISR, RPA or UAS equipment in support of the State CD mission requires separate SecDef approval. For example, the use of an MQ-9 Reaper RPA to support the State plan requires separate approval under reference hh.

b. Support for CD Activities and Activities to Counter Transnational Organized Crime – DoD Support. When approved by the SecDef or delegee, the T32 NG intelligence component may provide intelligence support to Federal agencies, such as the Drug Enforcement Administration, under the authorities of reference t. This intelligence activity is subject to IO and must also comply with the provisions of reference ii. CD coordinators with personnel providing Federal intelligence support are required to establish and maintain IO programs. Guardsmen must also comply with the privacy rules governing the supported agency and the rules under which the assignment or detail was approved.

c. IO Programs. Only NG CD programs providing intelligence support under reference t are required to maintain an IO program.

5. NG Chemical, Biological, Radiological, and Nuclear Response Enterprise (CRE).

a. NG Weapons of Mass Destruction–Civil Support Teams, Chemical Biological Radiological, and Nuclear Response Force Packages, and Homeland Response Forces, collectively known as the CRE, advise and facilitate in areas that have been or may be attacked with suspected weapons of mass destruction agents, advise civilian responders on appropriate actions through on-site testing and expert consultation, and facilitate the arrival of additional State and Federal military forces. Generally speaking, these units perform non-intelligence activity and will comply with provisions IAW reference dd and reference ee concerning the handling of information related to NDAPs.

b. Intelligence personnel assigned to intelligence billets to provide intelligence support to these units have the mission and authority to support emergency response, to prepare for possible response, and to perform effective research, analysis, and threat assessment. Intelligence personnel will comply with the provisions contained in reference a and this manual.

c. While conducting operations, CRE units may incidentally or otherwise collect NDAP information. Upon completion of operations, all NDAP information must be purged, destroyed, deleted, or redacted from information systems or physical files before being used in after-action reports, Mission Termination Packets, or other follow-up reports IAW reference dd and reference ee.

6. Critical Infrastructure Protection–Mission Assurance Assessment Detachments. The detachments conduct all-hazard risk assessments of prioritized Federal and State critical infrastructure in support of the Defense Critical Infrastructure Program. Intelligence analysts may be assigned to these detachments to perform effective research, analysis, and threat assessment. Intelligence analysts will comply with the provisions of this manual and reference a.

7. Cyber Intelligence and ISR. T32 NG personnel assigned to cyber intelligence and cyber ISR units and billets are subject to this manual and reference a. This includes T32 National Guardsmen filling intelligence billets on NG Cyber Protection Teams and on NG Defensive Cyberspace Operations-Elements.

ENCLOSURE E

DOMESTIC IMAGERY

1. Domestic Imagery. Domestic imagery supports commander needs for training and operational requirements (such as IAA, including situational awareness and SAR). NG units may, at times, require access to newly collected or archived domestic imagery. Collecting imagery inside the U.S. raises policy and legal concerns that require careful consideration, analysis, and coordination with legal counsel. Therefore, NG intelligence component personnel should use domestic imagery only when there is a justifiable need to do so, and then only IAW reference a, reference e, and this manual.

a. Legal Concerns. NG domestic imagery users must be aware of the legal and policy concerns associated with domestic imagery, particularly of USPERs and private property. Individuals may be held personally liable for any violation of law or inappropriate use of domestic imagery.

b. Missions. IAW reference jj, domestic imagery may be collected during authorized missions for the following purposes:

(1) Exercises and Training.

(2) Personnel Recovery.

(3) Systems Testing, Engineering, Research and Development. Requirements for imagery include support of system calibration, algorithm or analytic development and training, or weapons systems development or training.

(4) Humanitarian Assistance.

(5) Disaster Readiness, Response, and Recovery.

(6) Security Vulnerability Assessments.

(7) Scientific and Environmental Studies.

(8) Maritime and Aeronautical Safety of Navigation.

(9) Defense Support of Civil Authorities when directed by the SecDef.

2. Domestic Imagery from National Satellites. The National Geospatial-Intelligence Agency is responsible for the policy, legal review, and approval of requests for the collection and dissemination of NGA-provided domestic imagery. IAW reference jj and reference kk, the NG intelligence elements must submit requirements for new collection to the National Geospatial-Intelligence Agency through NGB-J2 (for T32) or the gaining combatant command or major command (for T10). The requestor must define the requirements for domestic imagery, outline its intended use, and include a proper use

statement acknowledging awareness of legal and policy restrictions. Imagery from national satellites without linkage to additional identifying information that ties the information to a specific USPER is not considered USPI.

3. Domestic Imagery from Airborne Platforms. Follow the policy of the gaining combatant command, Service, or major command when in T10. An approved PUM or DILR must be on file with NGB-J2 (for T32) before airborne platforms can be tasked to collect domestic imagery under any of the following conditions:

a. The use of sensors to collect data.

b. The use of intelligence analysts, systems, or organizations to process and exploit, analyze, and disseminate sensor data collected by airborne platforms.

c. The use of sensor data collected by airborne platforms for any purpose identified in paragraph 1.b. above by the T32 NG.

d. Refer to Table 4 for help in determining whether a PUM or DILR is required. This includes Government off-the-shelf and commercial off-the-shelf equipment.

Type of Asset	Type of Activity	Required Document
Intelligence Component Capability (for example, MC-12, MQ-9, RQ-28)	T10 Intelligence activity (for example, ISR for FI/CI purposes)	Follow gaining Service or Combatant Command policy
Non–Intelligence Component Capability (for example, A-10, F-15, F-16, UH-60, or UH-72)	T10 Intelligence activity (for example, non-traditional intelligence, surveillance, and reconnaissance for FI purposes)	Follow gaining Service or Combatant Command policy
Intelligence Component Capability (for example, , MC-12, MQ-9, RQ-28)	T32 Intelligence-related activity (for example, ISR training)	PUM
Non–Intelligence Component Capability (for example, A-10, F-15, F-16, UH-60, or UH-72	T32 Intelligence-related activity (for example, training for non-traditional intelligence, surveillance, or reconnaissance)	PUM
Intelligence Component Capability (for example, MC-12, MQ-9, RQ-20, RQ-28)	Non-intelligence activity (for example, IAA)	PUM
Non–Intelligence Component Capability (for example, A-10, Black Hornet, F-15, F-16, R80D SkyRaider, Soldier Borne Sensor (SBS) UH-60, or UH-72)	Non-intelligence activity (for example, IAA)	DILR

Table 4. Domestic Imagery Collection Documentation

4. CD PUMs and DILRs. PUMs and DILRs are not required for domestic imagery collection missions flown in support of a law enforcement agency under the approved State CD plan so long as the following three criteria are met:

a. The equipment being used for CD missions is operated by aircrews on CD-funded orders and is not ISR, UAS, or RPA equipment (such as MC-12, MQ-9, or RQ-28). Use of any ISR, UAS, or RPA equipment for CD purposes requires SecDef approval.

b. The analysis of the images collected is done by Service members on CD-funded orders or the supported law enforcement agency in support of the State CD mission.

c. The data or imagery is collected in support of the approved State CD plan and provided to the supported LEA, who owns and controls the data or imagery.

However, the use of UH-72 sensors for other purposes, such as IAA or SAR, likely requires a DILR. All DILRs must be filed IAW paragraph 6 below.

5. Domestic Imagery from Commercial Satellites.

a. NG intelligence component elements may access archived National Geospatial-Intelligence Agency domestic commercial satellite imagery (for example, Global Enhanced GEOINT Delivery [G-EGD] system) when supporting a valid Federal mission requirement, such as training or testing on Federally owned and operated ranges, calibration-associated systems development activities, homeland defense, and Defense Support of Civil Authorities in either T10 or T32 status. NG intelligence component elements may also use domestic publicly available and other commercial imagery (for example, U.S. Geological Survey imagery). States may request commercially available imagery through the NGB-J2 Operations, Plans, and Training Division (NGB-J23). The obligation of compliance with IO and other policies is with the user. An internal MFR describing the purpose of the domestic imagery collection and certifying proper use will be retained on file in all cases. A template for the MFR is provided in Figure 5. The NG intelligence component element may only collect, process, analyze, assess, or disseminate commercial imagery or imagery-associated products supporting their approved mission.

b. Imagery from commercial satellites without linkage to additional identifying information that ties the information to a specific USPER is not considered USPI. If obtained imagery specifically identifies a USPER, then follow the rules in Procedures 2 through 4 of this manual and reference e. Pay particular attention to procedures regarding retention. Reference jj and reference kk contain additional information on commercial satellite imagery use.

[Print on State letterhead]

[Insert Date]

MEMORANDUM FOR RECORD

Subject: [INSERT YEAR and UNIT (NGB-J2 202X)] Commercial Domestic Imagery and Other Geospatial Information Use Authorization

1. (CUI) In accordance with Chief of the National Guard Bureau Manual 2000.01, "The Conduct and Oversight of National Guard Intelligence Activities," Enclosure F, paragraph 5, this represents the [INSERT UNIT] memorandum of authorization to collect commercial imagery and produce imagery products for a one-year period. This authorization also includes commercially available and publicly available geospatial information and imagery products derived from commercial imaging sensors. Sources used include [[INSERT SPECIFIC DATABASES AND SYSTEMS USED BY THE UNIT] (*for example, ArcGIS, Domestic Operations Awareness and Assessment Response Tool, Google Earth, the Department of Homeland Security's Homeland Security Information Network, Homeland Security Infrastructure Program Gold, National Geospatial Intelligence Agency Net-Centric Geospatial Intelligence Discovery Services, NextView and Digital Globe, and U.S. Geological Survey EROS Hazards Data Distribution System)*.]

2. (U) This annual memorandum authorizes imagery and geospatial intelligence information collection, exploitation, retention, and dissemination in support of *INSERT UNIT* missions for the purposes of *INSERT THE PURPOSE FOR WHICH THE UNIT USES THE COMMERCIAL DOMESTIC IMAGERY AND OTHER GEOSPATIAL PRODUCTS [for example, military training, exercises, defense support of civil authorities, incident awareness and assessment, joint intelligence preparation of the operational environment, vulnerability assessments, and other incident support]*.

3. (U) The [INSERT UNIT] will be the primary end user of the imagery and geospatial information products; [[INSERT ANY OTHERS WHO MAY USE THE UNIT PRODUCTS AND HOW THE PRODUCTS WOULD BE DISSEMINATED TO THEM] *(For example, other local, State, and Federal agencies may request support from time to time. The imagery and information may be disseminated using hard or softcopy methods including shared enterprise portals such as National Guard Bureau Joint Intelligence Directorate SharePoint, , Defense Collaboration Services, and web-based data services; the Domestic Operations Awareness and Assessment Response Tool Server; Google Earth Enterprise Globe; U.S. Geological Survey Hazards Data Distribution System; the Department of Homeland Security Homeland Security Information Network; North American Aerospace Defense Command–U.S. Northern Command Sage Portal; North American Aerospace Defense Command–U.S. Northern Command full-motion video server; email; or hand delivery.)]*

4. (CUI) "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, 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."

Figure 5. Internal MFR Certifying Proper Use of Commercial Domestic Imagery

6. Manned and Unmanned Aircraft Navigational and Target Training Activities.

a. NG units with weapon system video and tactical ISR capabilities may collect imagery during formal and continuation training missions as long as the collected imagery is not for obtaining information about specific U.S. persons or private property. Collected imagery may incidentally include U.S. persons or private property without consent. For example, imagery may be collected of a private structure so that the imagery can be used as a visual navigational aid or to simulate targeting during training. Imagery may not be collected to gather any specific information about a USPER or private entity, without consent, nor may stored imagery be retrievable by reference to a USPER's identifiers.

b. NG fighter, bomber, remotely piloted aircraft, and unmanned aircraft systems operations, exercises, and training missions will not conduct surveillance on any specifically identified USPERs without consent, unless expressly approved by the SecDef, IAW U.S. law and regulations. Civilian law enforcement agencies, such as U.S. Customs and Border Protection, the Federal Bureau of Investigation, U.S. Immigration and Customs Enforcement, and the U.S. Coast Guard, will handle all such data.

c. A critical component of NG sensor operator training is preparing crews to conduct missions in deployed locations, which includes the ability to track mobile objects in both urban and rural settings. NG personnel are not authorized to retain data acquired during these training missions, nor will this data be disseminated in any form, unless otherwise required by law or policy and subject to servicing JA review. Intelligence component capability aircraft will follow Procedure 3 of reference e and this manual, aircraft conducting non-intelligence activity will follow reference dd and reference ee. To enable this training, airborne assets equipped with electro-optical, infrared, synthetic-aperture radar, or moving-target indicator sensors may perform visual reconnaissance of random vehicles on public roadways, without consent, during training missions under the following conditions:

(1) All training activities of this nature are supported by an applicable PUM or DILR that addresses the activity in detail as prescribed in this enclosure.

(2) Proper approval authority and other applicable permissions (for example, Federal Aviation Administration approval) for the training have been acquired.

(3) Sensors will not be used to gather, or attempt to gather, information that could lead to identifying a specific USPER or the person's identifiably unique features.

(4) Visual tracking of objects may be conducted only on public roadways or public lands. No tracking will be conducted in or around residences, businesses, or private property.

d. The use of NG UAS and RPA must comply with the policy in reference hh and reference ll.

7. PUMs, DILRs, and Commercial Domestic Imagery Internal Memorandums for Record.

a. PUMs and DILRs.

(1) PUMs and DILRs do not constitute the approval authority for the underlying T32 or authorized State Active Duty training, exercise, or operation.

(2) PUMs and DILRs are an entity's notice of collection, processing, analysis/assessment, use, retention, and dissemination of domestic imagery for a certain purpose. PUMs and DILRs certify that:

(a) 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.

(b) The request for imagery is not for the purpose of targeting any specific USPER without their consent, nor is it inconsistent with the Constitutional and other legal rights of U.S. persons.

(c) Applicable security regulations and guidelines, and other restrictions will be followed.

(3) PUMs and DILRs can be classified or unclassified, depending on content. The PUM or DILR is written on the organization's letterhead and signed by the organization's certifying official, a field-grade officer, or the civilian equivalent, who will verify and remain accountable for the accuracy of the domestic imagery request. Failure to file a PUM before conducting a domestic imagery collection mission is a QIA, reportable IAW procedures established in reference i.

(4) Any NG JFHQs-State that are assigned or have operational control over NG assets that conduct domestic imagery activities as defined in paragraph 1.b. above are responsible for drafting and seeking approval for a PUM or DILR before executing a domestic imagery collection mission. In a T32 status, the NG JFHQs-State J2 will route PUMs and DILRs to NGB-J2 as outlined in paragraph 6.a(6) below. NGB-J2 will forward the PUM or DILR to NGB-GC for review. Once the document is found to be legally sufficient, NGB-J2 will approve the PUM or DILR and notify the requesting State. In a T10 status, the gaining combatant command or major command J2, Air Force Director of Intelligence (A2), or Army Director of Intelligence (G2) is responsible for the PUM or DILR, if one is required.

(5) A PUM or DILR may be written as a one-time or one-year request. One-year requests cover:

(a) Routine DoD training and exercises with all DoD manned and unmanned aircraft, excluding MQ-1C and MQ-9 in routine training areas. Authorized State training and exercises with DoD UAS in State Active Duty require separate a PUM or DILR.

(b) Routine MQ-1C and MQ-9 training and exercises. Authorized State training and exercises with DoD UAS/RPA in State Active Duty require a separate PUM.

(c) SAR missions.

(d) IAA missions.

(6) Current PUM and DILR templates are available for download on the NGB-J2-IO website, reference u. PUMs and DILRs will include the following:

(a) Subject Line. Identify the document as an NG T32 or State Active Duty PUM or DILR for a domestic imagery request. Include the date(s) on which collection will occur.

(b) Paragraph 1. References. Include all applicable intelligence oversight or NDAP information protection and domestic imagery policy documents. Add State IO standard operating procedures to all PUMs.

(c) Paragraph 2. Tasking and Collection. Use nontechnical terms in the purpose of the request, the intended use of the imagery, the timeframe for collection, where the collection will occur, what the sensors will image, the airborne platforms and sensors to be used, and whether SIGINT, HUMINT, or measurements and signatures intelligence (MASINT) will be collected or disseminated (include authorities if any SIGINT, HUMINT, or MASINT will be collected).

(d) Paragraph 3. USPER or NDAP Statement. Include either:

1. The following statement: “No U.S. persons (PUMs) or non-DoD affiliated persons (DILRs) will be targeted during these missions. Any personally identifying information unintentionally and incidentally collected about specific U.S. persons (PUMs) or non-DoD affiliated persons (DILRs) 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.”

2. If a USPER (PUM) or NDAP (DILR) will be targeted or collection of imagery is focused on a specific residence or non-Federal entity, further review and documentation may be required IAW laws and policy. Consult with your State JA and NGB-J2 prior to such collection.

(e) Paragraph 4. Processing and Exploitation, Analysis and Dissemination. Specify the organizations and equipment that will process and exploit, analyze, and disseminate the imagery and sensor data, and for what purpose. Exploitation tasks and activities are limited to training in the domestic environment. Include the organizations that are to receive the imagery (or derived products, briefings, or publications) and the desired format; retention information (where the imagery will be stored); disposal procedures; and certification that IO (PUMs or NDAP information protection policy (DILRs)) training has been given.

1. Identify each user organization, even if a large number of organizations are involved. Using the product in briefings and publications will require additional review if the audience goes beyond the original request in the PUM or DILR.

2. Request the format of the imagery (for example, digital, tape, paper, or print).

3. If the requested imagery will be loaded onto an automated information system, include the system's name.

(f) Paragraph 5. State Army Aviation Officer Review. Include the following statement: "The information regarding the Army NG Aviation assets in this PUM or DILR was reviewed for accuracy by the State Army Aviation Officer. [insert Army State Aviation signature block and signature]"

(g) Paragraph 6. Judge Advocate Review. Include the following statement: "This PUM or DILR for domestic imagery was reviewed for legal sufficiency by the [applicable State JA or component legal office (for example, California National Guard, or Vermont National Guard Office of the Staff Judge Advocate) with [JA contact information] for compliance with law, policy, and intelligence oversight. [insert JA signature block and signature]"]

(h) Paragraph 7. Proper Use Statement and Certification by NG JFHQ-State J2. This must be an officer in the rank of Major or higher, Chief Warrant Officer 3 or higher, or civilian equivalent Government Grade (GG)- or General Service-13 (GS)-13 or higher. Usually, this is the NG JFHQs-State J2. If the NG JFHQ-State J2 does not meet the rank requirement, an official with the appropriate rank who will be accountable for the accuracy of the domestic imagery request and ensure the requested imagery and derived products are maintained IAW this manual and other applicable policy is authorized to sign. Certification wording is either:

1. "I certify that the intended collection and use of the requested information, materials, and imagery are in support of Congressionally approved programs and do not violate applicable laws or policy, including the statutory authority of [insert organization]. The request for imagery is not for the purpose of targeting any specific USPER (PUMs) or non-DoD affiliated person (DILRs), 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."

2. "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 herein and for the proper safeguarding of products received in response." Insert the rank and name of the certifying official and his or her contact information. This must be an officer in the rank of Major or higher, Chief Warrant Officer 3 or higher, or civilian equivalent GG/GS-13 or higher.

(i) Paragraph 8. Point of Contact Information. Name, office, telephone number, and email address or fax number for the PUM or DILR point of contact.

(j) Signature authority. The signature of the certifying official.

(7) Staffing procedures for T32 airborne platform PUM and DILR rules:

(a) Approval resides with NGB-J2.

(b) Requests will be submitted using email to NGB-J2 at <ng.ncr.arng.list.ngb-j2-intel-oversight@army.mil>. PUMs or DILRs for routine training and exercises should be sent to NGB-J2 no later than 15 working days before the first day of collection.

(c) In a direct and immediate emergency there may not be time to obtain an approved PUM or DILR before collection. TAG or the CG may authorize airborne domestic imagery collection, including the lawful acquisition of USPI (PUMs) or NDAP information (DILRs) when that support is consistent with reference h and other laws, regulations, and instructions. The NG JFHQs-State must implement the proper safeguards to protect all information and products collected, acquired, received, or used during emergency response and ensure that all applicable security regulations and guidelines and other restrictions are followed. In such cases, a report will be made immediately to NGB-J2 through the NG Joint Operations Center. A PUM or DILR will be filed with NGB-J2 as soon as possible thereafter.

(d) NGB-J2 will coordinate all PUM and DILR reviews and approvals with NGB-GC to ensure legal sufficiency.

(e) The NGB-J2 IO Section will provide a copy of all relevant PUMs and DILRs to the applicable combatant command or major command, as necessary, for situational awareness.

b. Commercial Domestic Imagery Proper Use Internal MFR. The MFR describes the purpose of the collection, retention, or dissemination of commercial satellite, publicly available, and other commercial domestic imagery and other geospatial data. The intelligence organization's certifying official will sign the MFR, approving the collection and use of the imagery. The MFR must be retained on file one year after its expiration. It may be recertified if the imagery is still required. See Figure 5, or the NGB-J2 IO website, reference u for a template.

7. Dissemination of Domestic Imagery.

a. Distribution of domestic imagery to parties other than those identified in the approved PUM or DILR is prohibited unless the recipient is reasonably believed to have a specific, lawful governmental function requiring it. Adding users to the original PUM or DILR is accomplished by submitting an amendment to the PUM or DILR. See the NGB-J2 IO website, reference u for a PUM or DILR amendment template. Domestic imagery used in briefings, reports, or publications may not be used for any purpose other than that for which it was originally requested.

b. Unless otherwise approved, domestic imagery must be withheld from all general access database systems. Controlled or limited access shared folders or drives, password-protected websites, password-protected portals, and email distribution are acceptable means for disseminating or providing access to domestic imagery to authorized users. Applicable security and classification requirements must be met. The intent is to provide a reasonable assurance that the entire user group on a general-access Web system (for example, the DOMOPS Awareness and Assessment Response Tool, Intelink or the Secret Internet Protocol Router Network cannot access domestic imagery without an appropriate authorization or control measure. Access must be limited to those with a need to know.

8. Processing and Exploitation, Analysis, and Dissemination of Domestic Imagery.

a. Domestic imagery adjacent to named areas of interest (targets of collection) incidentally acquired during execution of an approved PUM or DILR will not be analyzed unless approval is granted IAW the PUM or DILR process (that is, through approval of an amendment to the original PUM or DILR).

b. Domestic airborne imagery saved in historical files or on servers cannot be analyzed or used beyond the purpose identified in the original PUM or DILR without obtaining appropriate authorization through an amended PUM or DILR.

c. A requesting organization must clearly communicate in its PUM or DILR who the analysis and exploitation, if applicable, entities are, if they are different from the requesting organization.

d. Each organization is responsible for ascertaining and complying with any restrictions that may limit or prevent analysis or exploitation, if applicable, of imagery of a sensitive Federal named area of interest.

e. IAW reference mm and reference nn, National Guardsmen may not use Google Drive™, Gmail, or other non-military or commercial media for official collection or processing, analysis, and dissemination.

9. Public Affairs Use of Domestic Imagery.

a. Media and public interest in NG DOMOPS, including IAA, can be intense and immediate. Personnel will refer all media inquiries and other requests for information, including imagery, from outside the NG to the Public Affairs Officer.

b. While much of the imagery collected by NG units may be unclassified, that does not necessarily mean that it can be released to the public. All imagery must be reviewed by the NG JFHQs-State J2 to ensure no sensitive military or Government facilities are visible. Imagery released to private citizens and U.S. media will not include imagery of DoD installations or other sensitive areas. These sites can vary from general military installations to nuclear power plants. Releasing imagery of these types of facilities to the public or on an open website also releases the imagery to entities that wish to harm the United States. Once imagery is released to the public, the NG and

DoD no longer have any control over its use or dissemination. Therefore, all imagery will be reviewed, and its contents verified to confirm the need for release and to confirm that the right level of information is released to proper organizations IAW the PUM or DILR. Specific imagery products may be released to the U.S. media during senior officer press conferences to show disaster areas and disaster response activities.

c. IAW their policies, civil authorities are authorized to show, or release selected unclassified, Controlled Unclassified Information (CUI), or For Official Use Only (FOUO) imagery products to participating or affected private citizens when it would prevent injury or loss of life or facilitate disaster mitigation and recovery efforts.

ENCLOSURE F

INTELLIGENCE SUPPORT TO FORCE PROTECTION

1. General. NG intelligence component support to FP may involve identifying, researching, reporting, analyzing, and disseminating intelligence regarding foreign threats to the NG, thereby enabling commanders to initiate FP measures. If during the course of routine activities and authorized missions, NG intelligence component personnel receive information (including information identifying USPERs) regarding threats to life or property (whether DoD personnel, installations or activities, or civilian lives or properties), then that information must be passed to appropriate authorities.

a. FP operations within the United States are the primary responsibility of civilian Federal, State, Territorial, Tribal, and local law enforcement authorities. In the United States, the NG intelligence component will limit FP activities to FI and international terrorism threat data. The NGB and NG JFHQs-State Provost Marshal or law enforcement branch, or NGB-J34 provide NG leadership with information and recommendations to support decision-making pertaining to FP, critical infrastructure, security, and law enforcement activities. This activity requires review, analysis, and distribution of significant and relevant law enforcement information. The NGB, NG JFHQs-State Provost Marshal or law enforcement branch, and NGB-J34 may receive and disseminate time-sensitive threat information within the United States, regardless of source or type. As non-intelligence entities, they are not subject to the provisions of this manual but must comply with reference dd and reference ee.

b. When foreign groups or persons threaten DoD personnel, resources, or activities, the NG intelligence component may report on this information.

c. Law enforcement agencies and other organizations or sources may disseminate information that contains USPI to the NG intelligence component. It is important to remember that information is collected upon receipt (see Procedure 2 in reference e and Enclosure B of this manual). Follow retention and dissemination rules in Procedure 3 and Procedure 4 in reference e and Enclosure B of this manual. Intelligence professionals are obligated to go back to any disseminating agency that routinely provides USPI for which they have no mission and authority to cease further dissemination of such products and to direct the dissemination to the appropriate office (such as NGB-J34, Provost Marshal Office, or other law enforcement branch).

d. IO provisions do not prohibit States from having meetings or establishing “information fusion cells” or “threat working groups” where representatives from intelligence, CI, security, and law enforcement meet to share and combine information to support the FP mission. Security, FP, or law enforcement--not intelligence personnel--should lead the meeting.

e. Consolidated (intelligence and criminal data) threat assessments cannot be filed, stored, or maintained as an intelligence product. These assessments must be filed, stored, and maintained within operational channels. NG intelligence component

elements will not control FP databases within the U.S. NG intelligence component elements that are assigned an FP mission must handle USPI only IAW the procedures in reference e and this manual.

2. Dual-Hatting Intelligence, FP, or Provost Marshal Personnel. Personnel in NG intelligence positions (such as the NG JFHQs-State J2) will not be dual-hatted as the NG JFHQs-State J34, Provost Marshal, or Force Protection Officer. A clear separation between intelligence, FP, and Provost Marshal channels must be maintained. Consolidated databases and files are not permitted. This paragraph does not apply to National Guard personnel who have different jobs as Technicians and in drill status and use different systems, email accounts, and offices for each. For example, an individual may be the NG JFHQs-State FP Officer as a Technician and be a Brigade Intelligence Noncommissioned Officer in drill status.

3. Reporting Incidentally Acquired Threat Information.

a. If, during the course of routine activities and authorized missions, NG intelligence component personnel receive information that includes USPI on potential threats to life, limb, or property, then the information must be passed to appropriate authorities IAW Procedure 4 of reference e and Enclosure B of this manual. Receipt of USPI does not constitute QIA or an IO violation. Intelligence personnel will route such information and ensure that it enters the proper channels.

b. If there is an imminent threat to life, limb, or potentially serious property damage, then the NG intelligence component will immediately notify the appropriate entities (for example, the post or base command section, Military Police, Security Forces, Provost Marshal, the Federal Bureau of Investigation, or the municipal police department) with authority to counter the threat.

c. Without an imminent threat, reporting should be limited to NG JFHQs-State J34, Provost Marshal, or other law enforcement branch, which will forward the information to other authorities as appropriate.

d. Threat information may be withheld from dissemination only upon the approval of the Director of Intelligence (Army) G2 or Director of Intelligence (Air Force) A2 for FI or Army Counterintelligence Command or the Commander, Air Force Office of Special Investigations, for CI, and only for National security reasons.

ENCLOSURE G

THE INTERNET AND PUBLICLY AVAILABLE INFORMATION

1. General.

a. NG intelligence component elements must have official mission requirements before collecting, using, retaining, or disseminating information, including publicly available information, about USPERs. In addition, IAW Procedure 10 of reference e and Enclosure B of this manual, certain Internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation.

b. To properly apply IO provisions to the use of the Internet, personnel conducting FI and CI activities must understand how to analyze and characterize Internet Protocol (IP) addresses, Uniform Resource Locators (URLs), and email addresses IAW reference qq.

2. IP Addresses. Like a telephone number, the numeric string composing an IP address does not, without further information, identify or consist of information about a USPER. However, open-source information found on the World Wide Web, may in certain circumstances, allow for the linking of IP addresses to specific USPER. Generally, NG intelligence and CI components are not required to try to decipher an IP address as soon as they encounter one, but they are required to conduct an inquiry once a decision is made to conduct analysis that focuses on specific IP addresses. Prior to such analysis, IP addresses are treated as "data acquired by electronic means" and is not considered collected until it has been processed into intelligible form. There are no IO restrictions on maintaining or disposing of information that has not been "collected."

a. Once the decision is made to analyze specific IP addresses, the responsible NG intelligence component is obligated to conduct a reasonable and diligent inquiry to determine whether any of the IP addresses are associated with USPERs. If the NG intelligence component is unable to reasonably determine whether a given IP address is associated with a USPER, then there is a presumption that unattributed IP addresses do not constitute information about a USPER and may be handled accordingly. However, if the NG intelligence component subsequently obtains information indicating that an IP address is associated with a USPER, this presumption is overcome, and the IP address must be handled IAW the procedures governing the collection of USPI. A determination that an IP address is assigned to a U.S. internet service provider is not necessarily sufficient information to presume that the address is associated with a USPER. In the same way that a telephone number provides more information about the caller than about the telephone company, the IP address gives more information about the individual connection than about the internet service provider that provides the connection.

b. Some Internet service providers primarily serve a U.S.-based clientele. An IP address within a block assigned to such an Internet service provider may allow for the

presumption that the IP address within the assigned block is associated with a USPER . Conversely, if a group of IP addresses is known to be assigned to a non-USPER (for example, a foreign corporation), then the NG intelligence component may presume that the IP address is associated with a non-USPER. The NG component collecting this information should document their efforts determining whether the IP address in question is associated with a USPER.

3. Email Addresses. Email addresses, unlike both IP addresses and URLs, are nearly universally associated with individuals or organizations. However, it is often difficult to identify the individual with whom any given email address is associated. Some email addresses are configured as a string of alphanumeric symbols that do not convey any meaningful information (for example, smitgj@ or smi2345@). Others appear to plainly identify an individual (for example, George.Smith@). Regardless of how straightforward an email address appears to be, it usually does not provide sufficient information to identify it as being affiliated with a USPER. Sometimes, the name to the left of the "@" will provide persuasive evidence that the email address is associated with a USPER; for example, the email address may identify a well-known public figure or U.S. business or may be the target of an investigation or inquiry in which the intelligence investigator or analyst is engaged.

a. Occasionally, the information to the right of the "@" may provide persuasive evidence about whether an email address is associated with a USPER. Some internet service providers predominately serve a non–U.S.-based clientele, and email accounts with such providers may be presumed to be non-USPERs' accounts. Other service providers are so closely affiliated with the U.S. that any email account with that provider should be presumed to be associated with a USPER (for example, <George.Smith@ ng.army.mil>). This latter category of email addresses may be collected, retained, or disseminated only IAW the requirements of reference e and reference oo.

b. All other email addresses may be treated in the same way as described for the treatment of IP addresses. Email addresses that are not self-evidently associated with USPERs may be acquired, retained, and processed by NG intelligence component elements, with the appropriate mission and authority, without assuming that any given address is associated with a USPER so long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the NG intelligence component must make a reasonable effort to determine whether the addresses are associated with USPERs. Unlike IP addresses, there is no central repository to assist the component in identifying specific email addresses. Instead, the component must rely on traditional methods to determine whether a given address is used by a USPER.

c. For email addresses that are cryptic, it may be nearly impossible for the NG intelligence component to make an accurate determination. In such instances, the component may presume that the email addresses do not identify USPERs. As with all presumptions, the component is under a continuing obligation to be alert to information that might overcome this presumption.

4. URL. In determining whether a URL identifies a USPER, a key factor to consider is the information to the right of the dot, known as the domain. If the domain is commonly associated with a foreign country (for example, .uk, .fr), then, in the absence of contrary information, the URL can be presumed to identify a non-USPER. Conversely, if the domain is associated with the U.S. (for example, .gov or .mil), then the URL should be presumed to be information that identifies a USPER. Several domains are universally available, such as .com, .net, and .org, and do not provide information about whether the URL identifies a USPER or a foreign person. The mere use of a name in association with a universally available domain is usually insufficient to trigger the presumption that the URL constitutes information that identifies a USPER. As with all information, if the URL can be definitively associated with a USPER, then the collection, retention, and dissemination of the URL name must be handled IAW IO procedures.

a. Unlike IPs and email addresses, URLs are publicly available. Therefore, even if they identify USPERs, lists of URLs may be maintained by NG intelligence component elements provided they are within the scope of an authorized FI or CI activity assigned to that component. NG intelligence component elements may also open the websites associated with such URLs if doing so is part of an authorized mission.

b. If the NG intelligence component element seeks to collect information beyond what is publicly available on the website, then it must make a reasonable effort to determine whether they are collecting on a USPER and, if so, comply with IO procedures.

5. Social Media Use.

a. National Guard personnel who have been appropriately assigned to support IAA, SAR, or other DOMOPS may monitor social media using general search engines or approved DoD social media tools, including DATAMNR™ First Alert feeds, to guide IAA general geographic information analysis, identify individuals in distress, and alert or refine SAR operations using personally identifiable information, including name, home address, personnel conditions, and phone numbers. This information may be retained for the duration of the DOMOPS to aid SAR. In this circumstance, consent is implied based on the assumption that the individual desires rescue. All personally identifiable information must be erased immediately following the conclusion of DOMOPS. DoD DATAMNR™ First-Alert accounts may be used by National Guard personnel with .mil email addresses in a T32 or a T10 duty status to support authorized DoD missions.

b. Under no circumstances may National Guard personnel use personal social media accounts for official purposes. Only general search engines or DoD-approved social media tools may be used. Consult with the appropriate JA or GC Office before using social media tools and other publicly available information applications.

ENCLOSURE H

INTELLIGENCE OVERSIGHT CONTINUITY BINDER

1. The IO Monitor will maintain the IO Continuity Binder for the unit.

2. The binder may be in electronic or hardcopy format. Unless otherwise indicated, records will be maintained for the period indicated in records management guidelines IAW reference pp. At a minimum, the binder will contain:

a. Appointment letters and NGB IO Monitor Certification Course training certificates for primary and alternate IO Monitors. The IO Monitor Certification Course serves as initial and annual IO training for IO Monitors.

b. IO Monitor duties and responsibilities.

c. Unit-tailored IO training.

d. IO training records (initial, annual, and pre-deployment) to be maintained for three years.

(1) Use Service-specific systems of record management for maintaining IO training records (that is, Digital Tracking and Management System Code 301-219-3459 Comply with Intelligence Oversight Regulations, Laws, and Executive orders for ARNG units).

(2) IO Monitors will ensure access to and validate completeness of training records.

e. Staff, Unit, or Organization-oriented IO Self-Inspection Checklist. This is created by using the applicable checklists in Enclosure I.

f. Self-inspection and inspection records to be maintained for three years.

g. QIA, S/HSM, and Federal crime-reporting processes and report formats.

h. Copies of any QIA, S/HSM, and Federal crime reports to be maintained for three years.

i. Annual file review certification MFR to be maintained for three years.

j. SecDef authorizations or other approval documents requesting intelligence support to law enforcement agencies and other civil authorities, and other intelligence support.

k. Copies of the references in Figure 6 below.

- Executive order 12333, 04 December 1981, “United States Intelligence Activities,” As amended by Executive orders 13284 (2003), 13355 (2004), and 13470 (2008)
- Department of Defense (DoD) Directive 5148.13, 26 April 2017, “Intelligence Oversight”
- DoD Directive 5240.01, 27 September 2024, “DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities”
- DoD Manual 5240.01, 08 August 2016, “Procedures Governing the Conduct of DoD Intelligence Activities”
- Army Regulation 381-10, 27 January 2023, “The Conduct and Oversight of U.S. Army Intelligence Activities”
- Air Force Instruction 14-404, 03 September 2019, “Intelligence Oversight”
- CNGB Instruction 2000.01D, 18 January 2022, “The Conduct and Oversight of National Guard Intelligence Activities,” Incorporating Change 1, 15 June 2023
- CNGB Manual 2000.01C, 21 March 2025, “The Conduct and Oversight of National Guard Intelligence Activities”
- CNGB Instruction 0700.00A, 29 July 2024, “National Guard Inspectors General” Incorporating Change 1, 27 September 2024
- State IO Standard Operating Procedures

Figure 6. References for IO Continuity Binder

ENCLOSURE I

COMPLIANCE INSPECTION GUIDANCE AND SELF-INSPECTION CHECKLISTS

1. NG units may be inspected by NGB, supported major or combatant command, Service, and the DoD Senior Intelligence Oversight Official inspectors.

a. The inspectors may request mission briefings from all intelligence and intelligence-related units and staffs to understand their mission and authorities and then discuss their activities to ensure that they are legal and proper. Inspectors may review IO programs, including IO Monitor appointment letters, State IO policy, training records, training materials, IO Continuity Binders, and mandatory reference documents (see Enclosure H of this manual). They may ask to review intelligence files (paper and electronic copy format) to ensure no unauthorized USPI has been retained and may interview personnel to ensure they understand IO policy and can apply policy to their State and Federal missions.

b. Interviews may include determining whether personnel are familiar with basic IO requirements (for example, what constitutes a USPER; what constitutes a QIA or S/HSM; what obligation personnel have to report QIA, S/HSM, and Federal crimes; to whom personnel should report QIA, S/HSM, or Federal crimes; that no retaliatory action can be taken for reporting QIA, S/HSM, or Federal crimes; and where to find applicable IO directives, regulations, and policies). All inspectors will provide a verbal out-brief upon completion of their inspection. Inspectors from the NGB and DoD Senior Intelligence Oversight Official's Office will follow up with a written report.

2. DoD SIO Official inspection requirements are contained in reference c. DoD SIO Official inspection checklists and other inspection information are available in reference c and on their website in reference qq.

3. All units, staffs, and organizations subject to IO will perform a self-inspection in the final quarter of the calendar year if they have not received an IO inspection in the current calendar year by an IG. Maintain a copy of inspection and self-inspection results in the IO Continuity Binder for a minimum of three years.

APPENDIX A TO ENCLOSURE I

PROCEDURE 1 SELF-INSPECTION CHECKLISTS

Inspection Item	**Yes or No**
1. Is all intelligence (T10) or intelligence-related activity (T32) consistent with applicable Department of Defense (DoD), Service, and National Guard policy? (CNGB Instruction 2000.01D, paragraph 4, and CNGB Manual 2000.01C, Enclosure A, paragraph 1.a.)	Yes or No
2. Have you engaged in any intelligence or intelligence-related activity for the purpose of investigating U.S. persons, or collected or maintained information about them, solely to monitor activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution and laws of the United States? (CNGB Manual 2000.01C, Enclosure A, paragraph 1.b.)	Yes or No
3. Have you engaged in any intelligence activity for the purpose of affecting the political process in the United States? (See reference e, DoD Manual 5240.01, paragraph 3.1.b.)	Yes or No
4. Do you host or participate in a shared repository?	Yes or No
a. If you are a host, do you regularly audit access to U.S. person information (USPI) to the extent practicable? (DoD Manual 5240.01, paragraph 3.1.b.(2))	Yes or No
b. If you are a host, do participants inform you in writing that their participation complies with all law, policies, and procedures applicable to the protection of USPI? (DoDM 5240.01, paragraph 3.1.b.(2))	Yes or No
c. If you are a participant, do you ensure that your access to and use of the shared repository complies with all law, policies, and procedures applicable to the protection of USPI? (DoDM 5240.01, paragraph 3.1.b.(3))	Yes or No
d. If you are a participant, have you identified to the host any access and use limitations applicable to the USPI it provides? (DoDM 5240.01, paragraph 3.1.b.(3))	Yes or No
e. If you are a participant and provide USPI to a shared repository and allow access to or use of USPI by other participants, do you do so only in accordance with Procedure 4 of DoD Manual 5240.01? (DoD Manual 5240.01, paragraph 3.1.b.(3))	Yes or No

Table 5. Procedure 1 Self-Inspection Checklist

APPENDIX B TO ENCLOSURE I

PROCEDURE 2 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Do you have a Title 10 intelligence collection mission? Is all information that you collect necessary for performing an authorized intelligence mission or function assigned to you in the appropriate duty status? (DoD Manual 5240.01, paragraph 3.2.c).	Yes or No
2. Does all U.S. person information that you collect fall into a category specified in DoD Manual 5240.01, paragraph 3.2.c.(1) through (13)?	Yes or No
3. Do you address circumstances where an entity or individual is voluntarily providing on a recurring basis U.S. person information that is not relevant to an authorized mission or function? (DoD Manual 5240.01, paragraph 3.2.(d))	Yes or No
4. Do you collect information for the purpose of monitoring activities protected by the First Amendment or other Constitutional rights or U.S. law? (DoD Manual 5240.01, paragraph 3.2.f.(2))	Yes or No
5. Do you, to the extent practicable, limit collection of non-publicly available information to no more information than is reasonably necessary? (DoD Manual 5240.01, paragraph 3.2.f.(3)(a))	Yes or No

Table 6. Procedure 2 Self-Inspection Checklist

APPENDIX C TO ENCLOSURE I

PROCEDURE 3 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Do you have a process to promptly evaluate for permanent retention U.S. person information (USPI) that you collect or that is voluntarily provided to you? (DoD Manual 5240.01, paragraph 3.3.c.)	Yes or No
2. Do you have a process to track the temporary retention of unevaluated USPI to ensure that maximum retention periods are not exceeded? (DoD Manual 5240.01, paragraph 3.3.c.)	Yes or No
3. Do you have a process to delete from your automated systems of records all USPI, including any information that may contain USPI, unless you determine that the information meets the standards for permanent retention, within the applicable temporary retention period? (DoD Manual 5240.01, paragraph 3.3.c.(7))	Yes or No
4. Has the Defense Intelligence Component Head or delegee approved an extended period beyond the baseline extension periods in Procedure 3? If so, is there documentation to establish that the retention was necessary to carry out an authorized mission of your organization; that the information was likely to contain valuable information that your organization is authorized to collect in accordance with Procedure 2; that your organization will retain and handle the information consistent with the protection of privacy and civil liberties; that enhanced protections were considered; and that legal and privacy and civil liberties officials were consulted? (DoD Manual 5240.01, paragraph 3.3.c.(5))	Yes or No
5. Do you have a process to determine whether USPI may be permanently retained based on a determination that the USPI is necessary for the performance of an authorized intelligence mission assigned to your organization and one of the following? a. The information was lawfully collected by your organization or disseminated by another intelligence component and meets a collection category specified in CNGB Manual 2000.01C, Enclosure A, paragraph 3.i. b. The information was lawfully collected by your organization or disseminated by another intelligence component and is necessary to understand or access foreign intelligence or counterintelligence.	Yes or No

Table 7. Procedure 3 Self-Inspection Checklist

c. The information is required for oversight, accountability, or redress; by law or court order; or by direction of the Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency, a Component Inspector General, or the Attorney General. (DoD Manual 5240.01, paragraph 3.3.e.)	Yes or No
6. Do you have a process to limit access to and use of USPI to employees with appropriate security clearances, accesses, and a mission requirement? (DoD Manual 5240.01, paragraph 3.3.(f)(1)(a))	Yes or No
7. When retrieving USPI electronically, do you have a process to ensure you use only queries or other techniques that are relevant to the intelligence mission or other authorized purposes? (DoD Manual 5240.01, paragraph 3.3.(f)(b)1)	Yes or No
8. When retrieving USPI electronically, do you have a process to tailor queries or other techniques to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent to the intelligence mission and purpose for the query? (DoD Manual 5240.01, paragraph 3.3.(f)(b)2)	Yes or No
9. When retrieving USPI electronically, do you have written procedures to document the basis for conducting a query of unevaluated information that is intended to reveal USPI? (DoD Manual 5240.01, paragraph 3.3.(f)(b)3)	Yes or No
10. Are all intelligence files and documents that contain USPI, whether in print or electronic format, or posted to an Internet website, marked with the USPI warning notice? (DoD Manual 5240.01, paragraph 3.3.f.(2) and CNGB Manual 2000.01B, Enclosure A, paragraph 3.c)	Yes or No
11. Do you review all electronic and hardcopy files at least once each calendar year to ensure that retention of USPI is still necessary to an authorized function, has not been held beyond established disposition criteria, and was not retained in violation of the established retention standard? (CNGB Manual 2000.01C, Enclosure A, paragraph 3.d.)	Yes or No
12. Do you maintain on file for three years in the Intelligence Oversight Continuity Binder an internal Memorandum for Record certifying the annual file review was conducted, no unauthorized USPI has been retained, and no unlawful or improper queries of USPI have been made? (CNGB Manual 2000.01C, Enclosure A, paragraph 3.d.)	Yes or No

Table 7, continued. Procedure 3 Self-Inspection Checklist

APPENDIX D TO ENCLOSURE I

PROCEDURE 4 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Have all intelligence component personnel who disseminate U.S. person information (USPI) received training on Procedure 4? (DoD Manual 5240.01, paragraph 3.4.c.)	Yes or No
2. Do you ensure that all USPI disseminated by the intelligence component falls within one of the designated categories identified in Procedure 4? (DoD Manual 5240.01, paragraph 3.4.c.)	Yes or No
3. Do you determine that a recipient of USPI has a reasonable need to receive the information for the performance of its lawful mission? (DoD Manual 5240.01, paragraph 3.4.c.)	Yes or No
4. Have you disseminated USPI to other Intelligence Community elements? If no, proceed to question 6.	Yes or No (If No, proceed to question 6.)
5. If you have disseminated USPI to other Intelligence Community elements, has the dissemination met the requirements in DoDM 5240.01, paragraph 3.4.c.(2)?	Yes or No
6. Have you disseminated USPI to other DoD elements?	Yes or No (If No, proceed to question 8.)
7. If you have disseminated USPI to other DoD elements, has the dissemination met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(3)?	Yes or No
8. Have you disseminated USPI to other Federal Government entities?	Yes or No (If No, proceed to question 10.)
9. If you have disseminated USPI to other Federal Government entities, has the dissemination met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(4)?	Yes or No
10. Have you disseminated USPI to any State, Territorial, Tribal, or local governments?	Yes or No (If No, proceed to question 12.)
11. If Yes, has the dissemination met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(5)?	Yes or No

Table 8. Procedure 4 Self-Inspection Checklist

12. Have you disseminated USPI to foreign governments? If Yes, has the dissemination to foreign governments or international organizations met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(6)?	Yes or No
13. Have you disseminated USPI to any Federal, State, Territorial, tribal, or local governmental entity, an international entity, or an individual or entity not part of a government and is it necessary for the limited purpose of assisting in carrying out an authorized mission or function?	Yes or No If No, proceed to question 15.)
14. If Yes, has the dissemination met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(6)?	Yes or No
15. Have you disseminated USPI to a Federal, State, Territorial, tribal, or local governmental entity, an international organization, or an individual or entity not part of a government because it is necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or a threat to the national security?	Yes or No (If No, proceed to question 17.)
16. If Yes, has the dissemination met the requirements in DoD Manual 5240.01, paragraph 3.4.c.(6)?	Yes or No
17. Have you disseminated a large amount of USPI that has not been evaluated to determine whether it meets the permanent retention standard? If so, did the Defense Intelligence Component Head or delegee approve, after notifying the Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency, the dissemination? (DoD Manual 5240.01, paragraph 3.4.d.)	Yes or No
18. Do you have written procedures to ensure that any improper dissemination or suspected improper dissemination of USPI is reported immediately upon discovery? (DoD Manual 5240.01, paragraph 3.4.h. and 3.4.i. and CNGB Manual 2000.01C, Enclosure A, paragraph 4.b.)	Yes or No
19. Has any dissemination of USPI not conformed to the conditions set forth in Procedure 4 of CNGB Manual 2000.01C. If Yes, has the Defense Intelligence Component Head approved the dissemination? (DoD Manual 5240.01, paragraphs 3.4.h. and 3.4.i. and CNGB Manual 2000.01C, Enclosure A, paragraph 4.b.)	Yes or No

Table 8, continued. Procedure 4 Self-Inspection Checklist

APPENDIX E TO ENCLOSURE I

PROCEDURE 5 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Do National Guard intelligence component elements with the mission and authority to conduct electronic surveillance for foreign intelligence and counterintelligence purposes do so only while in a Title 10 status? (DoD Manual 5240.01, paragraph 3.5. and CNGB Manual 2000.01C, Enclosure A, paragraph 5.)	Yes or No
2. Is all electronic surveillance for counterintelligence purposes conducted in accordance with regulations, instructions, and procedures approved by the Secretary of the Army (for the Army National Guard) or Secretary of the Air Force (for the Air National Guard), and contained in U.S. Signals Intelligence (SIGINT) directives (USSIDs)? (CNGB Manual 2000.01C, Enclosure A, paragraph 5.)	Yes or No
3. Are all requests to perform electronic surveillance, including computer network exploitation, for foreign intelligence collection or against U.S. persons abroad for foreign intelligence purposes, done so with the appropriate mission and authority? (DoD Manual 5240.01, paragraph 3.5. and CNGB Manual 2000.01C, Enclosure A, paragraph 5.)	Yes or No
4. Do you ensure that SIGINT cryptologic element activities are conducted in accordance with applicable USSIDs? (DoD Manual 5240.01, paragraph 3.5. and CNGB Manual 2000.01C, Enclosure A, paragraph 5.)	Yes or No
5. National Guard Bureau Joint Intelligence Directorate (NGB-J2) TSCM Team only: Do you conduct all activity in accordance with Department of Defense Manuals S-5240.05 and 5240.01? (DoD Manual 5240.01, paragraph 3.5.i.(2) and CNGB Manual 2000.01C, Enclosure A, paragraph 5.d.)	Yes or No
6. NGB-J2 TSCM Team only: Has any incidental collection of USPI without consent of those subjected to the surveillance met all the following conditions? That: a. It is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. b. The use of TSCM is limited in extent and duration to that necessary to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.	Yes or No

Table 9. Procedure 5 Self-Inspection Checklist

c. The use of TSCM has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken. d. If the use of TSCM constitutes electronic surveillance, as that term is defined in the Foreign Intelligence Surveillance Act, such countermeasures are not targeted against the communications of any particular person or persons. (DoDM 5240.01, paragraph 3.5.i.(2))	Yes or No
7. NGB-J2 TSCM Team only: When conducting TSCM activity, do you retain or disseminate only the information that is acquired in a manner that constitutes electronic surveillance as that term is defined in Foreign Intelligence Surveillance Act to protect information from unauthorized surveillance or to enforce Chapter 119 of Title 18 and Section 605 of Title 47 U.S. Code? (DoD Manual 5240.01, paragraph 3.5.i.(2))	Yes or No
8. NGB-J2 TSCM Team only: Do you destroy any information acquired when it is no longer required for these purposes or as soon as is practicable? (DoD Manual 5240.01, paragraph 3.5.i.(2))	Yes or No
9. NGB-J2 TSCM Team only: If USPI is acquired in a manner that does not constitute electronic surveillance as that term is defined in Foreign Intelligence Surveillance Act, do you retain and disseminate that USPI in accordance with Procedures 3 and 4? (DoD Manual 5240.01, paragraph 3.5.i.(2))	Yes or No
10. NGB-J2 TSCM Team only: Do you retain technical parameters of a communication (for example, frequency, modulation, bearing, signal strength, or time of activity) only in accordance with DoD Manual 5240.01, paragraph 3.5.i.(2)?	Yes or No

Table 9, continued. Procedure 5 Self-Inspection Checklist

APPENDIX F TO ENCLOSURE I

PROCEDURES 6 THROUGH 13 SELF-INSPECTION CHECKLISTS

Inspection Item	**Yes or No**
1. Do National Guard (NG) intelligence component elements with the mission and authority to conduct concealed monitoring for foreign intelligence and counterintelligence purposes do so only while in a Title 10 status? (DoD Manual 5240.01, paragraph 3.6) and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No
2. Is all NG authorized concealed monitoring for foreign intelligence or counterintelligence purposes conducted in accordance with regulations, instructions, and procedures approved by the Secretary of the Army (for the Army National Guard) or Secretary of the Air Force (for the Air National Guard)? (DoD Manual 5240.01, paragraph 3.6) and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No
3. Are NG intelligence component personnel who are authorized to conduct or approve concealed monitoring trained and certified? (DoD Manual 5240.01, paragraph 3.6 and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No
4. Do NG intelligence component personnel who are authorized to conduct or approve concealed monitoring understand the definitions of “counterintelligence,” “concealed monitoring,” “consent,” “Department of Defense facilities,” “foreign intelligence,” “reasonable expectation of privacy,” “United States,” “U.S. person,” and “U.S. person information”? (DoD Manual 5240.01, paragraph 3.6 and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No

Table 10. Procedure 6 Self-Inspection Checklist

Inspection Item	**Yes or No**
Do Army National Guard counterintelligence elements with counterintelligence investigative authority conduct non-consensual physical searches only in a Title 10 status? (DoD Manual 5240.01, paragraph 3.7 and CNGB Manual 2000.01C, Enclosure A, paragraph 6.)	Yes or No

Table 11. Procedure 7 Self-Inspection Checklist

Inspection Item	Yes or No
Do Army National Guard counterintelligence elements authorized to search and examine mail outside the United States do so only in a Title 10 status in accordance with Service policies? (DoD Manual 5240.01, paragraph 3.8 and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No

Table 12. Procedure 8 Self-Inspection Checklist

Inspection Item	Yes or No
Do all National Guard military intelligence and counterintelligence elements authorized to perform physical surveillance for foreign intelligence or counterintelligence purposes do so only while in a Title 10 status? (DoD Manual 5240.01, paragraph 3.9 and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No

Table 13. Procedure 9 Self-Inspection Checklist

Inspection Item	Yes or No
Do all National Guard military intelligence and counterintelligence elements authorized to perform undisclosed participation for foreign intelligence or counterintelligence purposes do so only while in a Title 10 status? (DoD Manual 5240.01, paragraph 3.10 and CNGB Manual 2000.01C, Enclosure A, paragraph 6)	Yes or No

Table 14. Procedure 10 Self-Inspection Checklist

Inspection Item	Yes or No
1. Do National Guard (NG) intelligence component elements secure Secretary of Defense approval prior to providing intelligence support to civilian law enforcement agencies (LEAs) and other civil authorities? DoDD 5240.01, and CNGB Manual 2000.01C, Enclosure A, paragraph 7)	Yes or No
2. Is all dissemination to civilian LEAs of incidentally acquired information reasonably believed to indicate a violation of law done so in accordance with Procedure 4 and security policy? Are any sensitive sources and methods protected? (DoDD 5240.01, and CNGB Manual 2000.01C, Enclosure A, paragraph 7)	Yes or No
3. Do NG intelligence elements providing analysis support to a civilian LEA under Title 10 U.S. Code Section 284 authorities comply with the privacy rules governing the agency and the rules under which the assignment or detail was approved? (CNGB Manual 2000.01C, Enclosure D, paragraph 4.b)	Yes or No

Table 15. Intelligence Support to Civilian Law Enforcement Agencies and Other Civil Authorities Self-Inspection Checklist

APPENDIX G TO ENCLOSURE I

EMPLOYEE CONDUCT SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Are all intelligence and intelligence-related activities conducted in accordance with all laws and applicable Department of Defense (DoD), Service, and National Guard Bureau policy? (DoD Manual 5240.01, paragraph 1.2., and CNGB Instruction 2000.01D, paragraph 4, and CNGB Manual 2000.01C, Enclosure A, paragraph 1.a.)	Yes or No
2. Is all Federal intelligence and intelligence, surveillance, and reconnaissance (ISR) equipment used for activities other than authorized foreign intelligence or counterintelligence (CI) activities and associated training only when approved by the Secretary of Defense or designee? (DoD Manual 5240.01, paragraph 3.1.a.(3) and CNGB Instruction 2000.01, paragraph 4.a.)	Yes or No
3. Do all National Guard (NG) personnel operating in a State Active Duty status refrain from engaging in DoD intelligence and CI activities? (CNGB Instruction 2000.01D, paragraph 4.d, 4.e, and 4.f.)	Yes or No
4. Do all NG personnel operating in a State Active Duty status refrain from using DoD intelligence and ISR equipment, such as the Joint Worldwide Intelligence Communications System or National or DoD CI and human intelligence (HUMINT) tools, such as the Counterintelligence/Human Intelligence Automated Tool Set or Counterintelligence/Human Intelligence Information Management System, or resources intended for CI and HUMINT activities, unless authorized by the Secretary of Defense or designee? (CNGB Instruction 2000.01D, paragraphs 4.d, 4.e, and 4.f.)	Yes or No
5. Do NG intelligence personnel reassigned to a non-intelligence mission refrain from using or accessing intelligence or ISR systems, resources, or equipment or CI National or DoD CI or HUMINT tools? (CNGB Instruction 2000.01D, paragraph 4.g.)	Yes or No
6. Have all employees of NG intelligence component elements received initial intelligence oversight training tailored to the unit, staff, or organization’s mission within 90 days of assignment or arrival? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.d. and CNGB Manual 2000.01C, Enclosure C, paragraph 1.b.(1))	Yes or No
7. Is training documented and the documentation retained for three years?	Yes or No

Table 16. Employee Conduct Self-Inspection Checklist

(CNGB Instruction 2000.01D, Enclosure A, paragraph 15.c. and CNGB Manual 2000.01C, Enclosure C, paragraph 2 and Enclosure H, paragraph 2.d.)	
8. Have employees of NG intelligence component elements received annual intelligence oversight training tailored to the unit, staff, or organization's mission? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.d and CNGB Manual 2000.01C, Enclosure C, paragraph 1.b.(21))	Yes or No
9. Is training documented and the documentation retained for three years? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.c. and CNGB Manual 2000.01C, Enclosure C, paragraph 2 and Enclosure H, paragraph 2.d.)	Yes or No
10. Do all employees of NG intelligence component elements carry out reporting responsibilities as described in Enclosure B of CNGB Manual 2000.01C?	Yes or No

Table 16, continued. Employee Conduct Self-Inspection Checklist

APPENDIX H TO ENCLOSURE I

NATIONAL GUARD JOINT FORCE HEADQUARTERS-STATE

THE ADJUTANTS GENERAL (TAGs) AND COMMANDING GENERAL (CG) OF THE DISTRICT OF COLUMBIA SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Is TAG or CG knowledgeable of all State intelligence and intelligence-related activities carried out in the State? (CNGB Instruction 2000.01D, Enclosure A, paragraph 10.a.)	Yes or No
2. Has TAG or CG appointed in writing experienced intelligence professionals to serve as NG JFHQs-State primary and alternate IO Monitors? Verify the military occupational specialty or Air Force specialty code of the primary and alternate IO Monitors. (CNGB Instruction 2000.01D, Enclosure A, paragraph 10.b.)	Yes or No
3. Has TAG or CG published State IO policy and procedures that meet the requirements of CNGB Instruction 2000.01D, Enclosure A, paragraph 10.c? (CNGB Instruction 2000.01D, Enclosure A, paragraph 10.c.)	Yes or No
4. Has TAG or CG received initial and annual IO training? (CNGB Instruction 2000.01D, Enclosure A, paragraph 10.d.)	Yes or No
5. Is TAG or CG familiar with IO procedures and assign tasks and missions IAW IO policy and guidance? (CNGB Instruction 2000.01D, Enclosure A, paragraph 10.e.)	Yes or No

Table 17. NG JFHQs-State J2 Self-Inspection Checklist

Inspection Item	**Yes or No**
1. Is the National Guard (NG) Joint Force Headquarters–State (NG JFHQs-State) J2 knowledgeable of all State intelligence and intelligence-related activities carried out in the State? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.a.)	Yes or No
2. Has the State J2 identified all intelligence staffs, units, and personnel performing intelligence and intelligence-related functions and ANG information operations staffs, units, and personnel within the State and verified compliance with appropriate directives? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.h.)	Yes or No
3. Has the State J2 established and maintained an effective intelligence oversight (IO) Program for all personnel assigned or attached to the NG JFHQs-State J2? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.d.)	Yes or No

Inspection Item	Yes or No
4. Are copies of the signed appointment memos posted in the NG JFHQs-State J2 workspaces and filed in the IO Continuity Binder? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.e.)	Yes or No
5. Have all NG JFHQs-State intelligence component personnel and Judge Advocate (JA) and Inspector General (IG) personnel with IO responsibilities received initial and annual IO training? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.f.)	Yes or No
6. Are all NG JFHQs-State intelligence component personnel, State IGs, and JA personnel with IO responsibilities familiar with IO statutory and regulatory guidance, including reporting responsibilities and all restrictions? (CNGB Instruction 2000.01D, Enclosure A, paragraphs 11.f., 12.b., and 13.a.)	Yes or No
7. Is IO training documented and is the documentation retained for three years?	Yes or No
8. Have all personnel assigned or attached to the NG JFHQs-State J2 who access or use U.S. person information received annual training on the civil liberties and privacy protections that apply to such information? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.g.)	Yes or No
9. Is this training documented and is the documentation retained for three years? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.c. and CNGB Manual 2000.01C, Enclosure C, paragraph 2 and Enclosure H, paragraph 2.d.)	Yes or No
10. Has the NG JFHQs-State J2, after consulting with the NG JFHQs-State JA, submitted proper use memorandums and domestic imagery legal reviews to the National Guard Bureau Joint Intelligence Directorate (NGB-J2) for all domestic imagery training, exercises, or operational missions flown in a Title 32 status? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.l.)	Yes or No
11. Are all NG JFHQs-State J2 electronic and hardcopy files reviewed at least once each calendar year to ensure that no unauthorized U.S. person information has been retained? Are memorandums for record (MFRs) documenting these file reviews maintained on file in the IO Continuity Binder for three years? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.m.)	Yes or No
12. Does the NG JFHQs-State J2 certify the proper use of all domestic commercial or publicly available imagery, such as U.S. Geological Survey imagery, Google Earth™ imagery, and Falcon View™ imagery, through an internal MFR? Are these MFRs maintained on file in the IO Continuity Binder for three years? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.n.)	Yes or No

Inspection Item	Yes or No
13. Does the NG JFHQs-State J2 consolidate quarterly IO reports from all intelligence organizations, units and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities and submit a consolidated IO report to the NG JFHQs-State IG every quarter? (CNGB Instruction 2000.01D, Enclosure A, paragraph 11.o.)	Yes or No

Table 18, continued. NG JFHQs-State J2 Self-Inspection Checklist

Inspection Item	Yes or No
1. Does the State IG receive initial and annual IO training and maintain a working knowledge of IO statutory and regulatory requirements, including reporting responsibilities and restrictions? (CNGB Instruction 2000.01D, Enclosure A, paragraph 12.b.)	Yes or No
2. Does the State IG inspect NG intelligence and intelligence-related activities in the state at least once every two years? (CNGB Instruction 0700.01A, Enclosure A, paragraph 9.k.)	Yes or No
3. Does the State IG report all QIAs, S/HSMs and Federal crimes to NGB-IG immediately.? (CNGB Instruction 0700.01A, Enclosure A, paragraph 9.k.)	Yes or No
4, Does the State IG investigate QIAs and S/HSMs within State established procedures to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies? (CNGB Instruction 0700.01A, Enclosure A, paragraph 9.k.)	

Table 19. NG State IG Self-Inspection

APPENDIX I TO ENCLOSURE I

NATIONAL GUARD COMMANDER, DIRECTOR, AND SENIOR INTELLIGENCE OFFICER (SIO) OF INTELLIGENCE OR INTELLIGENCE-RELATED ACTIVITY ORGANIZATIONS SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Is the Commander, Director, or SIO knowledgeable of the missions, plans, and capabilities of assigned and subordinate intelligence and intelligence-related capabilities and levying tasks and missions IAW IO policy and guidance? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.b.)	Yes or No
2. Has the Commander, Director, or SIO received initial and annual IO training? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.a.)	Yes or No
3. Has the Commander, Director, or SIO ensured that all required personnel assigned or attached to the organization receive IO training and are familiar with IO statutory and regulatory guidance, including the reporting responsibilities and all restrictions? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.e.)	Yes or No
4. Has the Commander, Director, or SIO established and maintained an effective IO program for all assigned or attached personnel? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.c.)	Yes or No
5. Has the Commander, Director, or SIO appointed in writing experienced intelligence professionals to serve as primary and alternate IO Monitors? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.d.)	Yes or No
6. Are copies of the signed appointment memos posted in the workspaces and filed in the IO Continuity Binder? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.d.)	Yes or No
7. Has the Commander, Director, or SIO ensured that all personnel assigned or attached to the organization who access or use U.S. person information are trained annually on the civil liberties and privacy protections that apply to such information? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.e.)	Yes or No

Table 20. NG Commander, Director, and SIO of Intelligence or Intelligence-Related Activity Organizations Self-Inspection Checklist

8. Has the Commander, Director, or SIO forwarded proposals for intelligence activities that may be questionable or contrary to policy to a servicing Judge Advocate or NG JFHQs-State Judge Advocate for review and submission to the Office of the National Guard Bureau General Counsel if required? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.g.)	Yes or No
9. Has the Commander, Director, or SIO ensured all personnel who report questionable intelligence activity allegations are protected from reprisal or retaliation? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.h.)	Yes or No
10. Has the Commander, Director, or SIO imposed appropriate sanctions upon any employees who violate the provisions of CNGB Instruction 2000.01 or other applicable policies? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.i.)	Yes or No
11. Has the Commander, Director, or SIO ensured that all electronic and hardcopy intelligence files are reviewed at least once each calendar year to ensure that no unauthorized U.S. person information has been retained and ensured that a memorandum for record is maintained on file in the IO Continuity Binder certifying that the review has been accomplished? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.j.)	Yes or No
12. Has the Commander, Director, or SIO certified the proper use of all domestic commercial or publicly available imagery, such as U.S. Geological Survey imagery, Google Earth™ imagery, and Falcon View™ imagery, through an internal memorandum for record at least once a calendar year and maintained the certifications in the IO Continuity Binder? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.k.)	Yes or No
13. Has the Commander, Director, or SIO submitted a quarterly IO report to the State Joint Intelligence Directorate? (CNGB Instruction 2000.01D, Enclosure A, paragraph 14.l.)	Yes or No

Table 20, continued. NG Commander, Director, and Senior Intelligence Officer of Intelligence or Intelligence-Related Activity Organizations Self-Inspection Checklist

APPENDIX J TO ENCLOSURE I

NATIONAL GUARD INTELLIGENCE OVERSIGHT MONITOR
SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Has the IO Monitor successfully completed initial and annual IO training through the NG IO Monitor certification course? (CNGB Manual 2000.01C, Enclosure C, paragraph 1.c.)	Yes or No
2. 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, and confirmed that personnel can identify, at a minimum, the purpose of the IO program; the regulations and instructions governing IO; IO rules affecting their mission; reporting procedures for questionable intelligence activity, significant or highly sensitive matter and Federal crimes; and the identity of the IO Monitors? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.b.)	Yes or No
3. Has the IO Monitor conducted IO training for all personnel within the staff, unit, or organization who require it, including intelligence personnel, other personnel conducting intelligence or intelligence-related activity, Judge Advocates, and Inspectors General in accordance with CNGB Manual 2000.01C, Enclosure D? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.c.)	Yes or No
4. Has the IO Monitor maintained records for three calendar years, including the dates personnel received training, for all IO training? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.c. and CNGB Manual 2000.01C, Enclosure C, paragraph 2 and Enclosure H, paragraph 2.d.)	Yes or No
5. Has the IO Monitor maintained an IO Continuity Binder in accordance with CNGB Manual 2000.01C, Enclosure I? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.d. and CNGB Manual 2000.01C, Enclosure I)	Yes or No
6. Has the IO Monitor maintained copies of State IO policy and applicable references so they are available to the organization? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.e. and CNGB Manual 2000.01C, Enclosure I)	Yes or No
7. 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 Inspector General from the DoD Senior Intelligence Oversight Official, major command, or National Guard Bureau? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.g.)	Yes or No

Table 21. National Guard Intelligence Oversight Monitor Self-Inspection Checklist

8. Has the IO Monitor assisted in making determinations on collectability of U.S. person information as detailed in Procedure 2, if required? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.h.)	Yes or No
9. Has the IO Monitor reviewed all files, electronic and paper, at least once per calendar year to ensure that any U.S. person information is retained in accordance with Procedure 3 and certified that all files have been reviewed through a memorandum for record and maintained on file in the IO Continuity Binder for three years? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.i.)	Yes or No
10. Does the IO Monitor know all reporting channels for questionable intelligence activity reports and reports of incidents or significant or highly sensitive matter and other federal crimes? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.j.)	Yes or No
11. Has the IO Monitor immediately routed questionable intelligence activity reports and reports of incidents, or significant or highly sensitive matter as specified in CNGB Instruction 2000.01D, Enclosure A, paragraph 15.j.?	Yes or No
12. Has the IO Monitor submitted a quarterly IO report through the chain of command to the State Inspector General? If you are an Air National Guard unit IO Monitor, have you provided a copy to the gaining major command, if required? (CNGB Instruction 2000.01D, Enclosure A, paragraph 15.k.)	Yes or No

Table 21, continued. NG Intelligence Oversight Monitor Self-Inspection Checklist

APPENDIX K TO ENCLOSURE I

NATIONAL GUARD INTELLIGENCE COMPONENT PERSONNEL
SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Do personnel understand the authorities and authorized mission of the organization to which they are assigned? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.a.)	Yes or No
2. Are personnel familiar with the policies contained in CNGB Instruction 2000.01D; Procedures 1 through 4 and policy for providing intelligence support to law enforcement agencies and other civil authorities; standards for employee conduct; procedures for reporting questionable intelligence activity, significant or highly sensitive matter, and Federal crimes; and any other procedures applicable to the assigned unit's mission or discipline? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.b.)	Yes or No
3. Do personnel conduct intelligence and intelligence-related activities in accordance with applicable law and policy, including CNGB Instruction 2000.01D and CNGB Manual 2000.01C and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.c.)	Yes or No
4. Have personnel completed the organization's IO training within 90 days of assignment or employment, as well as annual refresher training and pre-deployment IO training? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.d.)	Yes or No
5. Do personnel report any intelligence activity that may violate guiding laws or policies on questionable intelligence activity as well as significant or highly sensitive matter and Federal crimes to the U.S. Attorney General immediately upon discovery? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.e.)	Yes or No
6. Are personnel able to identify the organization's IO Monitor and do they know how to establish contact? (CNGB Instruction 2000.01D, Enclosure A, paragraph 16.f.)	Yes or No

Table 22. NG Intelligence Component Personnel Self-Inspection Checklist

.

ENCLOSURE J

THE INTELLIGENCE OVERSIGHT PROCESS

1. USPI may be intentionally collected by the least intrusive means possible if the intelligence component has the authorized mission or function to collect the information, the information is necessary to accomplish that mission or function, and the information falls in one or more of the 13 authorized categories listed in Procedure 2 of reference e.

2. Special collection techniques require additional approval. The flowchart in Figure 7 represents the decision-making process when considering how to handle USPI when conducting NG intelligence and intelligence-related missions and functions.

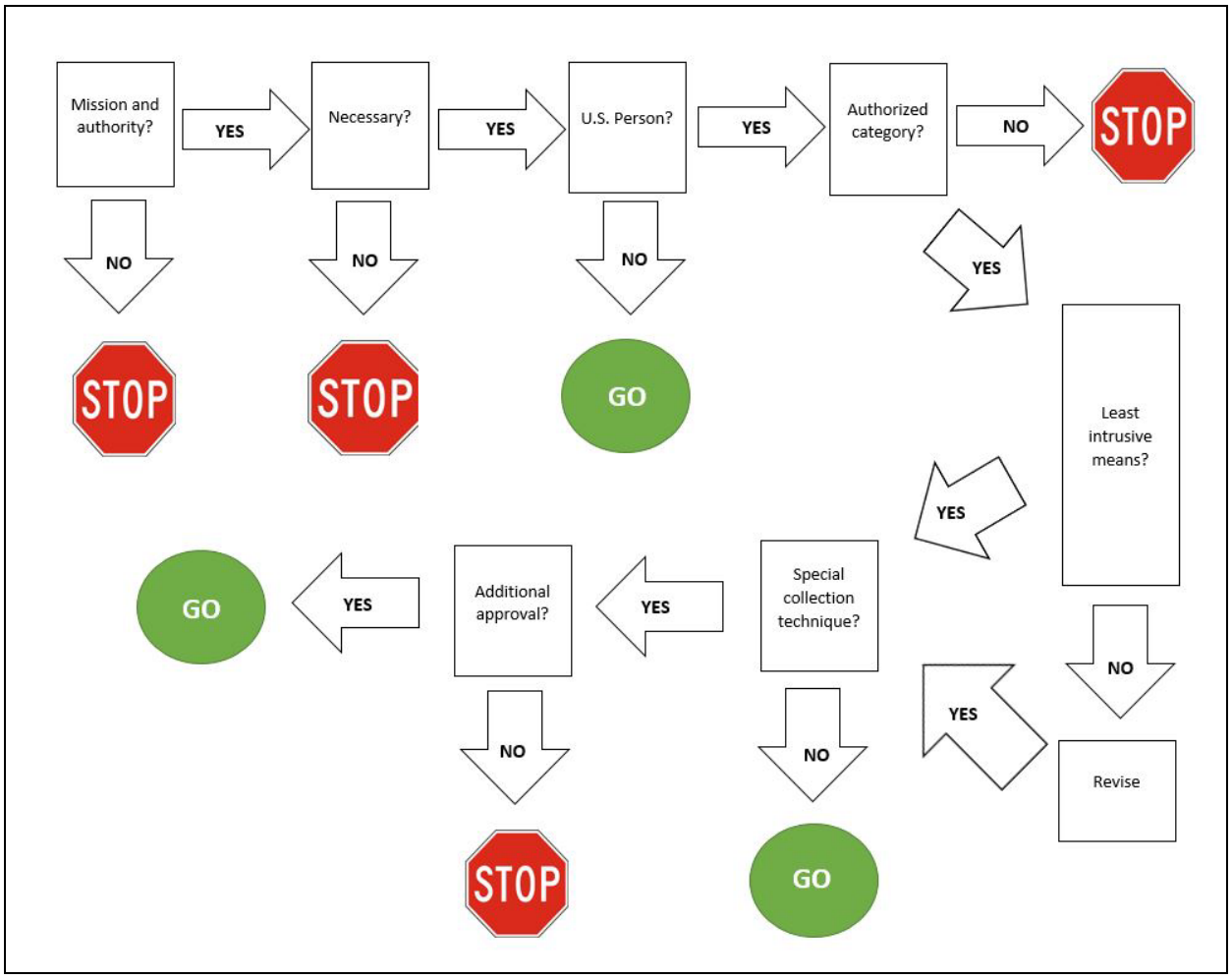

Figure 7. The Intelligence Oversight Process

3. Steps in working through the Intelligence Oversight Process are:

a. Step 1. Do you have the authority and mission to collect, process, analyze, retain, or disseminate the intelligence? If “No”, then stop; do not collect, process,

analyze, use, retain, or disseminate the intelligence. Your defined intelligence mission may be found in execute orders, operation orders, USSIDs, or SecDef memorandums.

b. Step 2. You have the authority and mission, but is collecting, processing, analysis, retention, or dissemination of the intelligence necessary to successfully carry out your defined mission, function, or task? If "No", then stop; do not collect, process, analyze, retain, or disseminate the intelligence.

c. Step 3. Is USPI involved? If "No", then collect, process, analyze, retain, or disseminate the intelligence. If USPI is involved, then continue to Step 4.

d. Step 4. Does the information to be collected, processed, analyzed, retained, or disseminated fall within one of the 13 authorized categories? If "No", then stop; do not collect, process, analyze, retain, or disseminate the intelligence. If "Yes", then continue to Step 5.

e. Step 5. Is the information to be collected by the least intrusive means possible? If "Yes", proceed with Step 6. If "No", revise the collection plan to the least intrusive means possible.

f. Step 6. Does the collection involve any special collection techniques? Special collection activities include electronic surveillance (Procedure 5), concealed monitoring (Procedure 6), physical searches (Procedure 7), searches of mail and use of mail covers (Procedure 8), physical surveillance (Procedure 9), undisclosed participation in organizations (Procedure 10), undisclosed contracting for goods and services for intelligence purposes, and any other activities that could be perceived by the general public as a covert surveillance and covert reconnaissance activity. If "No", then proceed with collection. If "Yes", then continue to Step 7.

g. Step 7. Seek additional approval required of special collection techniques and then proceed. Without approval, stop.

ENCLOSURE K

REFERENCES

PART I. REQUIRED

a. Chief of the National Guard Bureau (CNGB) Instruction 2000.01D, 18 January 2022, "The Conduct and Oversight of National Guard Intelligence Activities," Incorporating Change 1, 15 June 2023

b. Executive order 12333, 04 December 1981, "United States Intelligence Activities," as amended by Executive orders 13284 (2003), 13355 (2004), and 13470 (2008)

c. Department of Defense (DoD) Directive 5148.13, 26 April 2017, "Intelligence Oversight"

d. DoD Directive 5240.01, 27 September 2024, "DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities"

e. DoD Manual 5240.01, 08 August 2016, "Procedures Governing the Conduct of DoD Intelligence Activities"

f. Army Regulation 381-10, 27 January 2023, "The Conduct and Oversight of U.S. Army Intelligence Activities"

g. Air Force Instruction 14-404, 03 September 2019, "Oversight of Intelligence Activities"

h. Constitution of the United States of America, 04 March 1789, Amended 07 May 1992

i. CNGB Instruction 0700.00A, 29 July 2024, "National Guard Inspectors General" Incorporating Change 1, 27 September 2024

j. Presidential Policy Directive 28, 17 January 2014, "Signals Intelligence Activities"

k. United States Signals Intelligence Directives (USSID) SP0018 (S), 27 July 2003

l. USSID 1000, U.S. Army Cryptologic Missions – SIGINT Activities, 27 June 2022

m. USSID 1260, U.S. Army National Guard Expeditionary SIGINT Activities, 05 February 2015

n. USSID 3000 (Air Force) (U//FOUO), 17 October 2019

o. USSID SE 3500 (ANG) (S), 11 January 2013

p. USSID 3775 (ANG) (U//FOUO), 16 April 2015

q. USSID 1221, Exercise SIGINT (S), 20 August 2018, Revised 18 January 2019

r. Under Secretary of Defense for Intelligence and Security (I&S) Memorandum, 24 March 2014, “Request for Authority to Establish a Technical Surveillance Countermeasures Program (TSCM)”

s. DoD Manual S-5240.05, 23 April 2015, “(U) The Conduct of Technical Surveillance Countermeasures (TSCM),” Incorporating Change 2, 04 March 2017

t. 10 U.S.C. Section 284, “Support for Counter-drug Activities and Activities to Counter Transnational Organized Crime”

u. National Guard Bureau Joint Intelligence Directorate (NGBJ2) NIPRNET Intelligence Oversight Program website: <https://armyeitaas.sharepoint-mil.us/teams/NGB-J2-IO>, accessed 21 March 2025

v. Memorandum of Understanding Between the Attorney General and the Secretary of Defense, August 1995, “Reporting of Information Concerning Federal Crimes”

w. DoD Instruction 5240.04, 01 April 2016, “Counterintelligence (CI) Investigations,” Incorporating Change 2, 18 September 2020

x. Department of the Air Force Policy Directive 10-7, 22 June 2021, "Information Operations (IO)"

y. Air Force Instruction 10-701, 24 July 2019, “Operations Security (OPSEC)”

z. National Guard Bureau Intelligence Oversight Monitor Certification Course website: <https://www.milsuite.mil/university/ngb-j2-io-training/courses/national-guard-bureau-intelligence-oversight-monitor-certification-course/>, accessed 21 March 2025

aa DoD Senior Intelligence Oversight Official NIPRNET website: <https://dodsioo.defense.gov>, accessed 21 March 2025

bb. 32 U.S.C. Section 112, “Drug Interdiction and Counter-drug Activities”

cc. Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict Memo, 07 March 2022, “National Guard Counterdrug Program (CDP) Guidance”

dd. DoD Directive 5200.27, 07 January 1980, “Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense”

ee. CNGB Instruction 3000.07, 15 November 2023, “Acquisition and Storage of Information Concerning Persons and Organizations not Affiliated with the Department of Defense”

ff. CNGB Instruction 3100.01B, 06 March 2020, “National Guard Counterdrug Support Program

gg. CNGB Manual 3100.01, 20 July 2021, “National Guard Counterdrug Support”

hh. Secretary of Defense Policy Memorandum, 31 October 2023, “Guidance for the Use of Unmanned Aircraft Systems in U.S. National Airspace”

ii. Secretary of Defense Memorandum, 22 February 2021, “Department of Defense Counterdrug-Funded Analytical Support”

jj. National Geospatial-Intelligence Agency Instruction NGA 8900.5, 02 January 2020, “Domestic Imagery,” Incorporating administrative update, 09 March 2020

kk. National Geospatial-Intelligence Agency Instruction NGA 1806, 15 March 2019, “Domestic Imagery,” Incorporating administrative update, 15 January 2020

ll. CNGB Instruction 7500.00, 13 October 2016, “Domestic Use of National Guard Unmanned Aircraft Systems”

mm. DoD Instruction 8170.01, 02 January 2019, “Online Information Management and Electronic Messaging,” Incorporating Change 1, Effective 24 August 2021

nn. Deputy Secretary of Defense Memorandum, 16 January 2018, “Conducting Official Business on Electronic Messaging Accounts”

oo. DoD Office of General Counsel Memorandum, 06 February 2001, “Principles Governing the Collection of Internet Addresses by DoD Intelligence and Counterintelligence Components”

pp. CNGB Instruction 5001.01, 05 December 2016, “National Guard Bureau Records Management Program”

qq. DoD Senior Intelligence Oversight Official SIPRNET Websites, <SIPRNET: intellipedia.intelink.sgov.gov/wiki/Intelligence_Oversight_Inspections_and_Best_practices>, accessed 21 March 2025

rr. 32 U.S.C. Section 101, “Definitions”

ss. DoD Instruction 5505.01, 27 January 2012, “Titling and Indexing Subjects of Criminal Investigations in the Department of Defense”

tt. DoD Directive 5143.01, 24 October 2014, “Under Secretary of Defense for Intelligence and Security (USD(I&S)),” Incorporating Change 2, 06 April 2020

GLOSSARY

PART I. ACRONYMS

A2	Director of Intelligence (Air Force)
ARNG	Army National Guard
CD	Counterdrug
CG	Commanding General of the District of Columbia
CI	Counterintelligence
CNGB	Chief of the National Guard Bureau
CUI	Controlled Unclassified Information
CRE	Chemical, Biological, Radiological, and Nuclear Response Enterprise
DILR	Domestic imagery legal review
DoD	Department of Defense
DOMOPS	Domestic Operations
FI	Foreign intelligence
FI/CI	Foreign intelligence/Counterintelligence
FOUO	For Official Use Only
FP	Force protection
G2	Director of Intelligence (Army)
GC	General Counsel
HUMINT	Human intelligence
IAA	Incident awareness and assessment
IAW	In accordance with
IG	Inspector General
IO	Intelligence oversight
IP	Internet Protocol
ISR	Intelligence, surveillance, and reconnaissance
J2	Joint Director of Intelligence
JA	Judge Advocate
MASINT	Measurements and signatures intelligence
MFR	Memorandum for record
NDAP	Non-DoD affiliated person
NG	National Guard
NG JFHQs-State	National Guard Joint Force Headquarters–State
NGB	National Guard Bureau
NGB-GC	Office of the National Guard Burau Chief Counsel
NGB-J2	Joint Intelligence Directorate
NGB-J2-IO	Intelligence Oversight Section
NGB-J34	Antiterrorism and Critical Infrastructure Protection Branch
NSA	National Security Agency
PUM	Proper use memorandum
QIA	Questionable intelligence activity
RPA	Remotely Piloted Aircraft
SAR	Search and rescue
SecDef	Secretary of Defense

S/HSM	Significant or highly sensitive matter
SIGINT	Signals intelligence
SIO	Senior Intelligence Officer
T10	Title 10 United States Code
T32	Title 32 United States Code
TAG	The Adjutant General
TSCM	Technical surveillance countermeasures
UAS	Unmanned Aircraft System
URL	Uniform Resource Locator
USPER	United States person
USPI	United States person information
USSID	United States Signals Intelligence Directive

PART II. DEFINITIONS

Air National Guard -- The organized militia of the States, Territories, and the District of Columbia, active and inactive, that is an air force; is trained, and has its officers appointed, under the 16th clause of Section 8, Article I, of reference h; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference rr.

Army National Guard -- The organized militia of the States, Territories, and the District of Columbia, active and inactive, that is a land force; is trained, and has its officers appointed, under the 16th clause of Section 8, Article I, of reference h; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference rr.

Certifying Official -- A National Guard field-grade officer in the rank of Major or higher, Chief Warrant Officer 3 or higher, or civilian equivalent General Grade/General Schedule-13 or higher, who verifies with the State Aviation Officer and applicable units and remains accountable for the accuracy of the domestic imagery request. The official will ensure that the requested imagery and derived products are maintained in accordance with this manual and other applicable policy. This is normally the JFHQ-State J2.

Chief of the National Guard Bureau -- The head of the National Guard Bureau, which is a joint activity of the Department of Defense, who is the highest-ranking officer in the National Guard and the National Guard of the United States. The Chief of the National Guard Bureau serves as the principal advisor to the Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, on matters involving non-Federalized National Guard forces and on other matters as determined by the Secretary of Defense. The Chief of the National Guard Bureau also serves as the principal adviser to the Secretary of the Army, Secretary of the Air Force, Chief of Staff of the Army, and Chief of Staff of the Air Force on matters relating to Federalized forces of the National Guard of the United States and its subcomponents, the Army National Guard and Air National Guard of the United States.

Collection -- Receipt of information by a Defense Intelligence Component, whether it is retained by the Component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include information that only momentarily passes through a computer system of the Component; information on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner; information disseminated by other Components or elements of the Intelligence Community; or information that is maintained on behalf of another United States Government agency and to which the Component does not have access for intelligence purposes.

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

Criminal Investigation -- In accordance with reference ss, any investigation into alleged or apparent violations of law undertaken for purposes that include the collection of evidence in support of potential prosecution.

Department of Defense Intelligence Components -- All Department of Defense organizations that perform foreign intelligence or counterintelligence missions or functions, including the National Security Agency Central Security Service; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; the foreign intelligence and counterintelligence elements of the Active and Reserve components of the Military Departments, including the Coast Guard when operating as a service in the Department of the Navy; the offices and staff of the senior intelligence officers of the combatant command headquarters; and other organizations, staffs, and offices when used for foreign intelligence or counterintelligence activities to which Part 2 of reference b applies.

Domestic Imagery -- A likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, covering the States, Territories, and the District of Columbia, and possessions of the United States, to a 12-nautical-mile seaward limit of the land areas. The definition of domestic imagery includes the collection of domestic data suitable for generating a likeness or representation of any natural or manmade feature, to include Light Detection and Ranging, Overhead Persistent Infrared, and Synthetic Aperture Radar data. The definition of domestic imagery applies regardless of sensor or source and includes domestic imagery collected from space-based national intelligence reconnaissance systems; airborne platforms, unmanned aerial vehicles, or other similar means; commercial imagery; hand-held or other ground based collection; and foreign partner imagery. Domestic Imagery does not include imagery-based basemaps covering the States, Territories, the District of Columbia, and possessions of the United States, to a 12-nautical-mile seaward limit of the land areas of a resolution that is insufficient to identify specific United States persons on the ground.

Email Address -- An address that identifies a user so that the user can receive Internet electronic mail. An email address typically consists of a name to identify the user to the mail server, followed by "@" and the host name and domain name of the mail server.

Employee -- A person employed by, assigned or detailed to, or acting for an element of the National Guard Intelligence Component.

Espionage -- The crime of spying on the Federal Government or transferring state secrets on behalf of a foreign country. If the other country is an enemy, espionage may be treason, which involves aiding an enemy. The term applies particularly to the act of collecting military, industrial, and political data about one nation for the benefit of another.

Force Protection -- Preventive measures taken to mitigate hostile actions against Department of Defense personnel (including family members), resources, facilities, and critical information.

Foreign Connection -- A reasonable belief that the of a United States person is or has been in contact with, or has attempted to contact, a foreign person or a representative or agent of a foreign country, for purposes harmful to the national security interests of the United States; or when a reasonable belief exists that the United States person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power, or a representative or agent of a foreign power, for purposes harmful to the national security interests of the United States.

Foreign Intelligence -- Information related to capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

Homeland Defense -- The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats, as directed by the President.

Homeland Security -- A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur.

Imagery -- A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations).

Intelligence Activity -- All activities that Department of Defense intelligence Components are authorized to undertake pursuant to reference b. This includes intelligence activities by non-intelligence organizations.

Intelligence Component Capability – To determine whether an asset is an "intelligence component capability," or whether a non-IC asset is being used as an intelligence component capability, intelligence law practitioners use the "5 Ps" Test (People, Pipes, Process, Platforms, and Purpose):

People -- What is the mission of the unit -- intel, training, operational, or other? What money is used to fund the unit?

Pipes -- Are intelligence component systems being used to disseminate the product? For example, products hung on the Joint Director of Intelligence/Director of Intelligence (Air Force) portal or use of intelligence systems backbone such as the Joint Worldwide Intelligence Communications System to push products to clients)? What money is used to fund those systems?

Process -- Where is the information going? Is an intelligence component or its personnel being used to process, analyze, or create products from the data collected (for example, 601st Intelligence, Surveillance and Reconnaissance Division conduct the processing, exploitation and dissemination)?

Platforms -- Is the platform owned or operated by and intelligence unit? If not, is a non-intel platform being used for intelligence gathering? (for example, F-16 targeting pod used to collect ground information for the Commander's information sharing for Defense Support of Civil Authorities support)? What money is used to fund the equipment?

Purpose -- What is the purpose of the activity? Is it to gather intelligence? Is it to train? Is it a mission in support of civil authorities?

Intelligence Oversight Monitor -- An individual assigned to establish and implement intelligence oversight procedures and training programs, evaluate staff and unit personnel intelligence oversight knowledge, and resolve collectability determinations in consultation with the servicing Inspector General and legal advisor.

Intelligence-Related Activity -- Those activities that are not conducted pursuant to Executive order 12333, but use intelligence funding (for example, Military Intelligence Program or National Intelligence Program) are rebuttably presumed to be intelligence-related activities. The use of procedures or technology similar to intelligence activities to conduct activities that have separate authorities but are not intelligence activities under Executive order 12333 does not necessarily convert those separate activities into intelligence-related activities. Examples of non-intelligence-related activities include, but not limited to, operations security activities such as own-force monitoring; force protection; cyberspace surveillance and reconnaissance operations; activities involving sensor systems that are so closely integrated with a weapons system that their primary

function is to provide immediate-use targeting data; maintenance of technologies or systems; and the types of activities listed in Paragraph 3.1.a.(3) of Department of Defense Manual 5240.01 as well as research, development, testing, and evaluation activities and training conducted in support of those activities. The term intelligence-related activity also includes those activities that are not conducted pursuant to Executive order 12333, but involve the collection, retention, or analysis of information, and the activities' primary purpose is to: train personnel to perform intelligence duties or activities; conduct research, development, testing, and evaluation for the purpose of developing intelligence-specific capabilities; or conduct intelligence-related sensitive activities, as referred to in reference tt.

International Terrorist Activities -- Activities undertaken by, or in support of, terrorists or terrorist organizations that occur totally outside the United States or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

Internet Protocol Address -- A numeric string (for example, 149.122.3.30) that identifies a hardware connection on a network. The numeric string represents information about the owner, operator, or user of the hardware connection.

Mail Cover -- The non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter. In this context, a “recording” means a transcription, photograph, photocopy, or other facsimile of the image of the outside cover, envelope, or wrappers of mail matter. A mail cover does not include opening or examination of mail that constitutes a physical search.

Memorandum of Agreement -- A document that defines general areas of responsibility agreement between two or more parties, normally headquarters or major command-level components, and stipulates an amount of reimbursable cost -- what one party does depends on what the other party does. It may contain mutually agreed upon statements of facts, intentions, procedures, parameters, and policies for future actions and matters of coordination.

Memorandum of Understanding -- A document that defines areas of mutual understanding between two or more parties, normally headquarters or major command-level components, that does not stipulate cost reimbursements, but explains what each party plans to do; however, what each party does doesn’t depend on what the other party does. It may identify expectations of recurring support normally not exceeding three years.

National Guard -- Unless the context indicates otherwise, the term “National Guard” in this issuance means the National Guard Bureau, Army National Guard and the Air National Guard of the States, Territories, and the District of Columbia.

National Guard Bureau -- A joint activity of the Army National Guard and Air National Guard pursuant to reference rr. The Chief of the National Guard Bureau is under the authority, direction, and control of the Secretary of Defense.

National Guard Intelligence Component -- National Guard Bureau, Title 32 National Guard Joint Force Headquarters-State, Title 32 National Guard intelligence units and staff organizations, and Title 32 non-intelligence organizations that perform intelligence or intelligence-related activities. The National Guard Intelligence Component in Title 32 duty status under the command and control of the Governor has no inherent authority to conduct intelligence activity, which is a Federal matter.

National Guard Intelligence Component Element -- An individual part of the National Guard Intelligence Component, such as an intelligence staff.

Necessary to the Conduct of a Function Assigned to the Collecting Component -- For purposes of collection of information about a United States person pursuant to Procedure 2 of reference e, the requirement that the function be both an authorized intelligence activity (foreign intelligence or counterintelligence) and a mission delegated to that specific Department of Defense intelligence component.

Non-United States Person -- A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States is not a United States person. A person or organization outside the United States is presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the United States is presumed not to be a United States person unless specific information to the contrary is obtained.

Proper Use Memorandum -- A memorandum signed by an organization's Certifying Government Official that defines the organization's domestic imagery requirements and intended use and contains a proper use statement acknowledging awareness of the legal and policy restrictions regarding domestic imagery.

Questionable Intelligence Activity -- Any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive order, Presidential directive, Intelligence Community Directive, or applicable Department of Defense policy governing that activity.

Reasonable Belief -- When facts and circumstances are such that a reasonable person would hold that belief. Reasonable belief must rest on facts and circumstances that can be articulated; hunches or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. Intelligence professionals should seek advice from intelligence oversight officer, chain of command, or trained Judge Advocate for assistance in making determinations when necessary.

Shared Repository -- A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains for the use of a single Defense Intelligence Component, or those acting on its behalf, is not a shared repository.

Significant or Highly Sensitive Matter -- An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an executive order, Presidential directive, Intelligence Community Directive, or Department of Defense policy), or serious criminal activity by intelligence personnel that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential: Congressional inquiries or investigations, adverse media coverage, impact on foreign relations or foreign partners, systemic compromise, loss, or unauthorized disclosure of protected information.

Social Media -- Forms of electronic communication (such as websites for social networking and blogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).

Special Activities -- Activities conducted in support of national foreign policy objectives abroad that are planned and executed so the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.

Uniform Resource Locator -- A standard way of specifying the location of an object on the Internet, typically a webpage. A Uniform Resource Locator represents an address used on the World Wide Web. Typically, these appear as words rather than numbers and, while some Uniform Resource Locators are gibberish, most of them convey a modicum of information. In some instances, that information is of a character that ostensibly identifies a person (for example, George_Smith.com or USSTEEL.com). In other instances, the words in a Uniform Resource Locator do not convey, in any apparent way, information concerning persons (or example, Bicyclists.com).

United States Person -- A United States citizen. An alien known by the Defense Intelligence Component concerned to be a permanent resident alien. An unincorporated association substantially composed of United States citizens or permanent resident aliens. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person. A person or organization in the United States is presumed to be a United States 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-United States person, unless specific information to the contrary is obtained.

United States Person Information -- A United States person's name, nickname, alias, unique title, Social Security number, or other unique personal identifier. Potentially identifying information, such as an address, telephone number, or license plate number requiring additional investigation to associate it with a particular person does not, alone, identify a United States person. If several types of potentially identifying information exist about a United States person, which, when considered together, essentially identify the United States person, that collective information will be considered United States person identifying information. United States person information is either a single item or information combined with other items that is reasonably likely to identify one or more specific United States persons. Determining whether information is reasonably likely to identify one or more specific United States persons in a particular context may require a case-by-case assessment by a trained intelligence professional. United States person information is not limited to any single category of information or technology. It 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. It does not include references to a product by brand or manufacturer's name or the use of a name in a descriptive sense (for example, Chevrolet Camaro or Cessna 172) or imagery from overhead reconnaissance or information about conveyances (for example, automobiles, trucks, aircraft, or ships) without linkage to additional identifying information that ties the information to a specific United States person such as name, email address, address, telephone number, Internet Protocol address, Social Security number, physical description, driver's license number, date of birth, or place of birth.