



CHIEF OF THE NATIONAL GUARD BUREAU MANUAL

NGB-J2
DISTRIBUTION: A

CNGBM 2000.01B
24 August 2022

NATIONAL GUARD INTELLIGENCE ACTIVITIES

References: See Enclosure L.

1. Purpose. This manual provides procedural guidance for National Guard (NG) intelligence and intelligence-related activities in accordance with (IAW) references a through i.
2. Cancellation. This manual supersedes its previous edition, Chief of the National Guard Bureau Manual (CNGBM) 2000.01A, 11 April 2019, "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. This manual provides the 13 procedures and guidelines for employee conduct and for identifying, reporting, and investigating questionable intelligence activity (QIA) and significant or highly sensitive matters (S/HSMs) defined in reference e.
 - 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 Department of Defense (DoD) intelligence component concerned.
 - c. Procedures 11 through 13 regulate other aspects of DoD intelligence activities, including provision of assistance to law enforcement authorities.
 - d. Employees of the NG intelligence component will follow Guidelines for Employees and conduct intelligence and intelligence-related activities only IAW

UNCLASSIFIED

24 August 2022

references a through i, 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 (EO), 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.

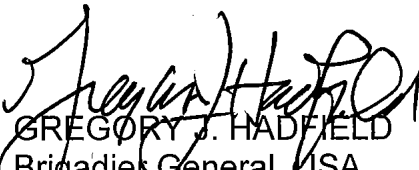
e. The NG intelligence component will also follow guidelines for identifying, reporting and investigating QIAs, S/HSMs, and Federal crimes. The NG intelligence component is required to report to the NGB Inspector General (NGB-IG) misconduct incidents to intelligence and intelligence-related activities that violate any EO, law, policy, or regulation governing those activities, S/HSM, and Federal crimes. Specific guidance is in Enclosure B.

f. Reference a and this manual do not authorize intelligence, CI, or intelligence-related activities. An NG intelligence component element must first have an approved mission, authority, and purpose before conducting the activity.

5. Summary of Changes. This document has been substantially revised. It reflects a significant change to DoD intelligence oversight (IO) policy, responsibilities, and procedures.

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 revised, reissued, cancelled, or certified as current every five years.



GREGORY J. HADFIELD
Brigadier General, USA
Director, Joint Intelligence

Enclosures:

- A -- Procedures
- B -- Identifying, Investigating, and Reporting Questionable Intelligence Activity, Significant or Highly Sensitive Matters, and Reportable Federal Crimes
- C -- Intelligence and Counterintelligence Disciplines and the National Guard
- D -- Intelligence Oversight Training Requirements
- E -- Domestic Operations
- F -- Domestic Imagery
- G -- Intelligence Support to Force Protection
- H -- The Internet and Publicly Available Information

I -- Intelligence Oversight Continuity Binder
J -- Compliance Inspection Guidance and Self-Inspection Checklists
K -- Intelligence Oversight Process
L -- References
GL -- Glossary

ENCLOSURE A

PROCEDURES

1. Procedure 1: General Provisions. All NG personnel will conduct intelligence and intelligence-related activities pursuant to reference b and only IAW references a and c through i, and this manual; personnel will not exceed the authorities granted by these references or by applicable laws, EOs, regulations, instructions, or policies. For the DoD, authorized intelligence activities are defense-related FI and CI conducted pursuant to reference b. The NG in Title 32, United States Code (T32) status trains to perform these missions. Intelligence activity in T32 status requires authorization by the Secretary of Defense or his designee. All intelligence and intelligence-related activities in all circumstances will be carried out IAW reference k and the laws of the United States.

a. Monitoring Activities. NG intelligence component elements may not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by reference k and laws of the United States. They 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. Furthermore, they will not participate in or request any person or entity undertake any activities that are forbidden by references b and d through f.

b. Shared Repositories of Data.

(1) Before granting access, an NG intelligence component element hosting a shared repository of data that may contain USPI will require each participant to acknowledge in writing completion of intelligence oversight training and agreement to comply with all laws, policies, and procedures applicable to the protection of USPI. A sample acceptable use agreement is shown in Figure 1. The NG intelligence component host will regularly audit access to USPI in the shared repository to the extent practicable to ensure that it meets the requirements for USPI collection, retention, and dissemination listed in Procedures 2 through 4 of this manual. Any QIA, as defined in reference c, discovered will be reported IAW Enclosure B. The NG intelligence component host is authorized to perform system support functions or data-related tasks, such as tagging, processing, or marking information, for itself or others. Access to USPI solely for these purposes does not constitute collection, retention, or dissemination.

<p style="text-align: center;">SAMPLE ACCEPTABLE USE AGREEMENT</p> <p>I acknowledge that my access to and use of <i>insert name of shared repository</i> complies with law, policies, and procedures applicable to protection of U.S. person information (USPI), including the intelligence oversight policy in Department of Defense Manual (DoDM) 5240.01 and Chief of the National Guard Bureau (CNGB) 2000.01 Issuance Series, "National Guard Intelligence Activities." I certify that any USPI I provide to the shared repository of data is consistent with Procedure 4 of DoDM 5240.01 and CNGB 2000.01 Issuance Series. Furthermore, I agree to notify <i>insert shared repository host's name</i> of any restrictions to access and use applicable to any USPI that I provide.</p>

Figure 1. Sample Acceptable Use Agreement

(2) NG intelligence component personnel accessing and using a shared repository must ensure that access to and use of the repository comply with law, policies, and procedures applicable to USPI protection (including this issuance) and must identify to the host any access and use limitations applicable to any USPI it provides. When NG intelligence component personnel using or contributing to a shared repository allow access to or the use of USPI, they have made a dissemination. Therefore, allowing access to or use of USPI in this manner will be conducted IAW Procedure 4 of this manual.

2. Procedure 2: USPI Collection.

a. USPI.

(1) USPI is information that is reasonably likely to identify one or more specific U.S. persons. It may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional or Judge Advocate (JA) professional.

(2) USPI is not limited to any single category of information or technology. USPI may include names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone number, and Internet Protocol address information. 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 U.S. person. Examples of USPI are shown in Table 1.

Name	Email Address
Address	Phone Number
Internet Protocol (IP) Address	Social Security Number
Physical Description	Driver's License Number
Date of Birth	Place of Birth

Table 1. Examples of USPI

b. Intentional Collection of USPI. The majority of intelligence professionals in the NG are all-source analysts without intelligence collection authorities. NG intelligence component elements may intentionally collect USPI only if it is reasonably believed to be necessary to perform an authorized intelligence mission or function assigned to the element and if the information falls within one or more of the following 13 categories below and in Table 2. All USPI must be collected by the least intrusive means possible.

Categories of Information
Publicly available information
Information obtained with consent
Information reasonably believed to constitute Foreign intelligence (FI)
Counterintelligence (CI)
Threats to safety
Protection of intelligence sources and methods
Current, former, or potential sources of assistance to intelligence activities
Persons in contact with sources or potential sources
Physical security
Personnel security
Communications security investigations
Overhead and airborne reconnaissance*
*A second category is required for collection under this category
Administrative purposes

Table 2. Categories of Information

(1) Publicly Available Information. Publicly available USPI includes information concerning U.S. persons appearing in print or electronic form, such as on the radio, on television, in newspapers, in journals, on the Internet, in commercial databases, and in videos, graphics, and drawings. An example is a Guardsman providing an intelligence briefing to his commander that includes information from the Internet regarding the commander of the Libyan National Army, U.S person (USPER) Khalifa Haftar.

24 August 2022

(2) Information Obtained with Consent. Information may be collected about U.S. persons who consent to such collection. An example is a U.S. person providing written consent to the NG for an MQ-9 Reaper to track him with the aircraft's sensors during a training mission. Consent is implied during search and rescue missions.

(3) Information Reasonably Believed to Constitute FI. USPI may be collected if the information is reasonably believed to constitute FI and the U.S. person meets one or more of the following descriptions:

(a) An individual reasonably believed to be an officer or employee of, or otherwise acting for or on behalf of, a foreign power.

(b) An organization or group reasonably believed to be directly or indirectly owned or controlled by, or acting on behalf of, a foreign power.

(c) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist or international narcotics activities.

(d) A corporation or other commercial organization reasonably believed to have some relationship with a foreign power, organization, or person.

(e) An individual reasonably believed to be a prisoner of war or missing in action; or an individual, organization, or group who is a target, hostage, or victim of an international terrorist or narcotics organization.

(4) CI. USPI may be collected if the information is reasonably believed to constitute CI, and the U.S. person meets one or more of the following descriptions:

(a) An individual, organization, or group reasonably believed to be engaged or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a foreign power, organization, or person, or on behalf of an agent of a foreign power, organization, or person.

(b) An individual, organization, or group reasonably believed to be engaged or preparing to engage in international terrorist activities or reasonably believed to be acting for or in furtherance of the goals or objectives of an international terrorist or international terrorist organization for purposes harmful to the national security of the United States.

(c) An individual, organization, or group in contact with a person described in the previous two paragraphs for the purpose of identifying such individual, organization, or group and assessing any relationship with each other.

(5) Threats to Safety. Information may be collected to protect the safety of any person or organization, including those who are victims, targets, or hostages of international terrorist organizations or individuals, when at least one of the following criteria is met:

(a) The threat has a foreign connection.

(b) The Defense Intelligence Component head or delegatee has determined that a person's life or physical safety is reasonably believed to be in imminent danger.

(c) The information is needed to maintain maritime or aeronautical safety of navigation.

(6) Protection of Intelligence Sources and Methods. Information concerning a U.S. person who has or had access to, or is otherwise in possession of, information revealing FI or CI sources, methods, or activities, may be collected when it is reasonably believed to be necessary to protect against the unauthorized disclosure of that information. Within the United States, intentional collection is limited to:

(a) Present and former employees.

(b) Present or former employees of a current or former contractor.

(c) Applicants seeking employment with the DoD or a DoD contractor.

(7) Current, Former, or Potential Sources of Assistance to Intelligence Activities. Information may be collected concerning those who are, have been, or are reasonably believed to be potential sources of information or assistance to intelligence activities for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

(8) Persons in Contact with Sources or Potential Sources. Information may be collected concerning persons in contact with a source or potential source for the purpose of assessing the suitability or credibility of such sources or potential sources.

(9) Personnel Security. Information arising from a lawful personnel security investigation may be collected.

(10) Physical Security. Information concerning a U.S. person who is reasonably believed to have a foreign connection and who poses a threat to the physical security of DoD employees, installations, operations, or visitors may be collected. USPI may also be collected in the course of a lawful investigation resulting from a physical security inspection, vulnerability assessment, or reported security incident. In all cases, the collector must be or have been supporting an authorized physical security mission and must be able to articulate a reasonable belief in the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.

(11) Communications security Investigation. Information arising from a lawful communications security inquiry or investigation may be collected.

(12) Overhead and Airborne Reconnaissance. Information may be obtained from overhead or airborne reconnaissance, including information from unmanned aircraft systems and remotely piloted aircraft and imagery from overhead (satellite) or

24 August 2022

airborne collection platforms operated commercially or obtained from other sources. A second category is required for collection under this category.

(a) NG intelligence component elements may intentionally collect imagery that contains USPI, provided that the collection is not directed at a specific U.S. person.

(b) Collection of any domestic imagery must also comply with other applicable laws, policies, and procedures, including DoD and National Geospatial-Intelligence Agency policy. See Enclosure F, "Domestic Imagery," for additional information.

(c) All collection of imagery must comply with Constitutional and statutory requirements, EOs, Presidential directives, and other provisions of this issuance.

(13) Administrative Purposes. Information may be collected as required for administrative purposes (for example, addresses and phone numbers for contact rosters).

c. Incidentally Collected USPI. In the course of authorized collection activities, NG intelligence component elements may incidentally collect USPI. Incidentally collected USPI may be temporarily retained to evaluate it for permanent retention and disseminated only IAW Procedures 3 and 4.

d. Voluntarily Provided USPI. Entities or individuals may voluntarily provide information to NG intelligence component elements on their own initiative. However, if an entity or individual is voluntarily providing on a recurring basis USPI that is not relevant to an authorized mission or function assigned to the NG intelligence component element, the NG intelligence component element will ask the entity or individual to cease doing so. If an element of the NG intelligence component reasonably believes that another NG entity, such as the Provost Marshal, has the lawful mission and function to receive the voluntarily provided information, the NG intelligence component element will redirect the information-holding entity or individual to the entity with the lawful mission and function instead. For example, if a law enforcement agency (LEA) continually provides the NG Joint Force Headquarters State (NG JFHQs-State) Intelligence Directorate (J2) with reports regarding the domestic criminal activity of U.S. persons, the NG JFHQs-State J2 must contact the LEA to be removed from the distribution list. If the NG JFHQs-State J2 reasonably believes the State Provost Marshal requires the information to carry out his assigned mission, then the NG JFHQs-State J2 can redirect distribution of the reporting to the State Provost Marshal.

e. Special Circumstances Collection.

(1) Special circumstances exist when any of the following criteria are met during collection opportunities: a large volume of USPI will likely be collected, the proportion of information collected is likely to be USPI, the type of USPI likely to be acquired is sensitive in nature, or an intrusive type of collection technique will be used.

24 August 2022

(2) The Defense Intelligence Component Head will review and approve all proposed special circumstances collection. If advance authorization is not possible, then, as soon as possible after collection, the Defense Intelligence Component Head must authorize the continued temporary retention of the information. The information must meet criteria in paragraphs 2.d(3)(a) and (b) below and Procedure 3. The Defense Intelligence Component Head consults the appropriate JA and appropriate officials responsible for the protection of civil liberties and privacy with any questions regarding whether special circumstances exist.

(3) An authorization of special circumstances collection will be based on both of the following:

(a) The information will be or has been properly collected IAW this procedure.

(b) The collection activity is reasonable based on all the circumstances, including the value of the information; the collection methods used; the amount of USPI; the nature and sensitivity of the USPI; the civil liberties and privacy implications of the collection; the potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed; and enhanced safeguards applied to the collected information.

(4) Figure 2 may be used to assist in determining whether special circumstances exist.

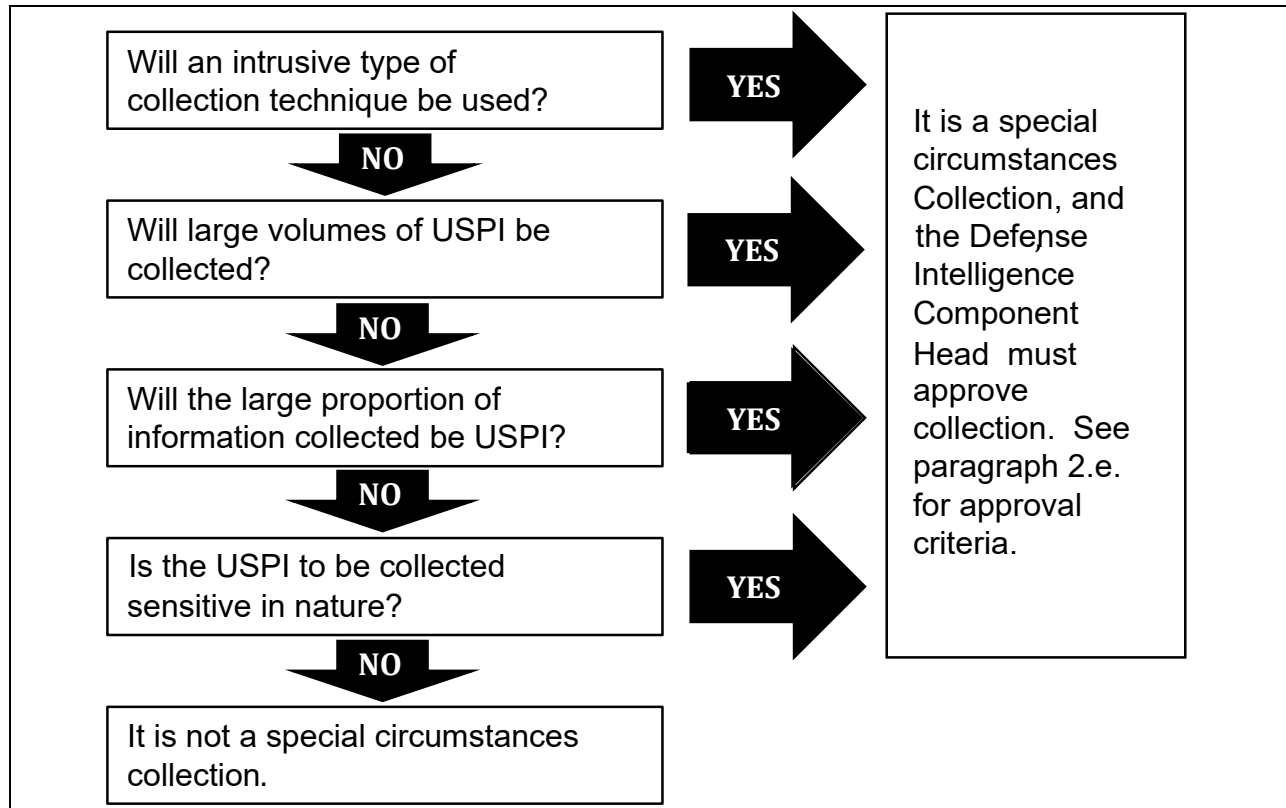


Figure 2. Does the Collection Constitute Special Circumstances Collection?

f. General Criteria Governing the Means Used to Collect USPI.

(1) Means of Collection. NG intelligence component elements with appropriate mission and authority in an appropriate duty status may collect USPI by any lawful means, provided that all such collection activities are carried out IAW references a through c.

(2) Restriction on Purpose. These NG intelligence component elements may not collect information solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by reference k or laws of the United States.

(3) Least Intrusive Means. These NG intelligence component elements will collect non-publicly available information by the least intrusive means possible and will collect no more information than is reasonably necessary to carry out their authorized mission.

(a) To the extent feasible, such information will be collected from publicly available sources or with the consent of the person concerned.

(b) If collection from publicly available sources or obtaining consent from the person concerned is not feasible or sufficient, such information may be collected from cooperating sources.

24 August 2022

(c) If collection from cooperating sources is not feasible or sufficient, such information may be collected using other lawful intelligence collection techniques that do not require a judicial warrant or the approval of the U.S. Attorney General.

(d) If collection from the three sources listed above is not feasible or sufficient, approval may be sought through the Defense Intelligence Component to the DoD General Counsel (GC) for the use of intelligence collection techniques that require a judicial warrant or approval from the Attorney General.

g. Limitations on FI Collection Within the United States. Within the United States, FI concerning U.S. persons may be collected subject to valid mission and authority only if at least one of these three conditions applies:

(1) The information is publicly available.

(2) The source of the information being collected is advised, or is otherwise aware, that the information is being provided to the DoD intelligence component.

(3) Other sources and methods within the authorized mission of the intelligence component are used and all of the following conditions are met:

(a) The FI sought is significant and must not be collected for the purpose of acquiring information concerning the domestic activities of any U.S. person.

(b) The FI cannot reasonably be obtained from publicly available information or from sources who are advised, or are otherwise aware, that they are providing information to the DoD intelligence component.

(c) The FI collection has been coordinated with the Federal Bureau of Investigation.

(d) The use of any other sources and methods has been approved by the appropriate Title 10, United States Code (T10) authority. A copy of any approval granted IAW this procedure will be provided through the Defense Intelligence Component to the Under Secretary of Defense, Intelligence and Security (USD(I&S)).

h. Date and Time Stamp. All USPI collected will be marked with the date and time it was collected in order to ensure that retention determination criteria outlined in Procedure 3 are met.

3. Procedure 3: USPI Retention. Intelligence component elements will evaluate all information that may contain USPI to determine whether it may be permanently retained.

a. Intentionally Collected USPI. Intelligence component elements will promptly evaluate all intentionally collected USPI to determine whether it meets the permanent retention standard. For the purposes of this manual, "promptly" is defined to mean as soon as is practically possible. If necessary, the intelligence component may retain the

USPI for evaluation for up to five years. The Defense Intelligence Component Head may approve an extended period IAW Paragraph 3.e. below.

b. Incidentally Collected USPI. In the course of routine duties, an NG intelligence component element may incidentally collect USPI. If the U.S. person to whom the incidentally collected USPI refers was inside the United States at the time of collection, the intelligence component element may retain all of the incidentally collected information for evaluation for up to five years. The Defense Intelligence Component Head may approve an extended period in accordance with paragraph 3.e. below. If the U.S. person to whom the incidentally USPI refers is reasonably believed to have been located outside the United States, the intelligence component element may retain all of the incidentally collected information for evaluation for up to 25 years.

c. Voluntarily Provided USPI. If an element of the intelligence component receives information that is voluntarily provided about a person reasonably believed to be a U.S. person, the intelligence component element will evaluate the information promptly. If necessary, the NG intelligence component element may retain the information for evaluation for up to five years. The Defense Intelligence Component Head may approve an extended period IAW paragraph 3.e. below. If an intelligence component element receives information that is voluntarily provided about a person reasonably believed to be a non-U.S. person, but the information may contain USPI, the intelligence component element may, subject to paragraph 3.e. below, retain the information for evaluation for up to 25 years.

d. Special Circumstances. If an intelligence component element conducts a special circumstances collection IAW Procedure 2.e., the intelligence component element may retain the information for evaluation for up to five years. If a special circumstances collection involves the intentional collection of USPI, that information will be promptly evaluated and, if necessary, may be retained for up to five years. Only the USD(I&S) may approve an extended period.

e. Evaluation Periods for Permanent Retention of USPI. Evaluation Periods for Permanent Retention of USPI are shown in Table 3.

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 USD(I&S) 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 3. Evaluation Periods for Permanent Retention of USPI

f. Extended Retention. The applicable Defense Intelligence Component Head, referred to as the “official” in paragraphs 3.e(1)(a), (b) and (c) below, may approve either at the time of collection or thereafter the further retention of specific information or categories of information subject to paragraphs 3.b, c, and d above for no more than five years beyond the time permitted in those paragraphs if:

(1) The official determines that retention is necessary to carry out an authorized mission of the intelligence component element, and the retaining intelligence component element will retain and handle the information in a manner consistent with the protection of privacy and civil liberties; considers the need for enhanced protection; and consults with legal and oversight officials.

24 August 2022

(2) In determining whether to approve an extended retention period, the official also finds that the information is likely to contain valuable information that the intelligence component element is authorized to collect IAW Procedure 2.

(3) The official must document compliance with the requirements of this paragraph in writing. Any further extension of retention beyond the limits specified in Paragraph 3.e must be addressed as an exception to policy IAW Paragraph 3.d.

g. Unintelligible Information. Periods for retention begin when information is processed into intelligible form. The intelligence component must process unintelligible information into intelligible form to the extent practicable.

h. Deletion of USPI. Intelligence component elements will delete all USPI, including any information that may contain USPI, that does not meet the permanent retention criteria from the intelligence component element's automated systems of records as soon as this determination is made or within the specified information evaluation period, whichever is sooner.

i. Information Disseminated by Another DoD Intelligence Component or Intelligence Community Element. An intelligence component element may retain information disseminated by another DoD intelligence component or Intelligence Community element and evaluate it for permanent retention only for as long as the originating agency is authorized to retain it. If the originating component or element has already determined that the information meets its standard for permanent retention, the intelligence component element must evaluate the information for permanent retention within a reasonable time.

j. Permanent Retention.

(1) Retention standard: NG intelligence component elements may permanently retain USPI if it determines that retention is reasonably believed to be necessary for the performance of an authorized mission or function and the USPI falls into one or more of these categories:

(a) The information was lawfully collected or disseminated to the NG intelligence component element by another DoD Intelligence Component or element of the Intelligence Community and meets a collection category in Procedure 2.a.

(b) The information was lawfully collected or disseminated to the NG intelligence component element by another DoD Intelligence Component or element of the Intelligence Community and is necessary to understand or assess FI or CI, such as information about a U.S. person that provides important background or context for FI or CI.

(2) Elements of the intelligence component may also retain USPI for purposes of oversight, accountability, or redress; when required by law or court order; or when directed by the DoD Senior Intelligence Oversight Official in the Office of the Assistant

to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (ATSD(PCLT)), a Component IG, or the U.S. Attorney General.

(3) NG intelligence component elements will maintain an internal memorandum for record (MFR) that documents the reason for permanently retaining any USPI and the authority approving the retention. A template is contained in Figure 3.

1. Description of USPI retained	
2. Date collected	
3. Type of collection (circle one)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	
<p>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.</p> <p style="text-align: right;">[J2/G2/A2/Senior Intelligence Officer (SIO)/Commander signature block]</p>	

Figure 3. Documenting Decisions to Permanently Retain USPI

k. USPI Protection. Limit access to and use of USPI to those employees who have appropriate security clearances, access, and mission requirement. When retrieving USPI electronically:

(1) Use only queries or other techniques that are relevant to the intelligence mission or other authorized purposes.

(2) 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.

(3) Document, on the internal MFR in Figure 4, the basis for conducting a query of unevaluated information that is intended to reveal USPI.

1. Date	
2. Database Queried	
3. USPI sought	
4. Authorized Mission Supported	
5. Describe why it is reasonably believed to be necessary to permanently retain the USPI	
6. Approved category(ies) of information under which the USPI falls (circle all that apply)	<ul style="list-style-type: none"> • 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 the purpose of targeting specific U.S. persons) • Administrative purposes
<p>I have approved the justification for conducting a database search for specific USPI and reasonably believe it is necessary for the conduct of an authorized mission, falls within an approved category of information and was properly collected.</p>	
<p align="right">[J2/G2/A2/senior intelligence officer (SIO)/Commander signature block]</p>	

Figure 4. Documenting Queries of Unevaluated Information Intended to Reveal USPI

I. Marking Electronic and Paper Files.

(1) Intelligence files and documents that contain USPI, whether retained in print or electronic format or posted to an Internet website, must contain a U.S. persons warning notice like the one contained in Figure 5.

“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 5. USPI Warning Notice

(2) This requirement applies whether or not the U.S. person is the subject of the collected information. 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. Intelligence component personnel must determine whether it is appropriate for intelligence products posted to the Internet 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 6.

“Other U.S. person information has been minimized. Should you require the minimized U.S. person information, please contact [insert office symbol and telephone number].”

Figure 6. 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 U.S. person.

(4) The first time a U.S. person 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 U.S. person appears in the product.

m. Annual File Reviews. NG intelligence component elements will review all electronic and hardcopy files at least once every 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 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 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 7 for a template.

[Day Month Year]
MEMORANDUM FOR RECORD
Subject: Annual File Review
Reference: Chief of the National Guard Bureau Manual 2000.01C, "National Guard Intelligence Activities"
1. I certify that, in accordance with Enclosure B, paragraph 3.I. of the reference, the [UNIT/STAFF] has reviewed all electronic and hardcopy files and no unauthorized U.S. persons information is being retained or held beyond established disposition criteria.
2. Point of contact for this is [NAME]; [PHONE].
[FIRST AND LAST NAME] [Rank, USA/USAF] [Commander/Director/SIO]

Figure 7. Annual File Review Certification Template

4. Procedure 4: Dissemination of USPI. The NG intelligence component may disseminate USPI information only IAW the following criteria:

a. The information was properly collected or retained IAW Procedure 2 and Procedure 3 above, and the pertinent information cannot be conveyed in an understandable way without including the identifying information. The information must also fall within one or more of the categories in Table 2.

b. The NG intelligence component employees disseminating the USPI have received training on this procedure. The disseminating NG intelligence component element will notify the recipient that the dissemination includes USPI, so the recipient can protect the USPI appropriately.

c. Refer to Table 4 for 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 4. 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 of 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; and (4) not disseminate the information further without the prior approval of the Defense Intelligence Component.

Table 4, 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 agreement approved by the Attorney General; or court order.	None

Table 4, continued. USPI Dissemination Categories with Criteria and Additional Rules

b. Disseminations Requiring Approval. Any dissemination that does not conform to the conditions set forth in this procedure must be approved by Director or Deputy Director of the NGB Joint Intelligence Directorate (NGB-J2) on the advice of the Office of the NGB General Counsel (NGB-GC) after consultation with the GC DoD. Such a determination will be based on a conclusion that the proposed dissemination complies with applicable laws, EOs, and regulations.

c. Applicability. Dissemination criteria apply equally to USPI in any form, including physical and electronic files and information the NG intelligence component places in databases, on websites, or in shared repositories accessible to other persons or organizations outside the NG intelligence component. It does not apply to information collected solely for administrative purposes or disseminated pursuant to other procedures approved by the U.S. Attorney General or a court order that otherwise imposes controls on such dissemination.

d. Improper Dissemination of USPI. Any improper dissemination or suspected improper dissemination of USPI will be reported immediately upon discovery IAW Enclosure B and Enclosure K.

5. Procedure 5: Electronic Surveillance.

a. Governing Principles. Section 1 of reference l lays out the governing principles for signals intelligence (SIGINT) collection. The National Security Agency (NSA) is the only organization that can authorize 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 kind of search covered by the Fourth Amendment to reference k. Units involved in SIGINT will be aware of and comply with applicable NSA/Central Security Service United States Signals Intelligence Directives (USSIDs) included in references m through t.

b. Mission and Authority. NG intelligence component elements with the mission and authority may conduct electronic surveillance for FI and CI purposes only while in a T10 status. Commands that have SIGINT cryptologic elements will ensure that those elements conduct activities IAW applicable USSIDs, such as references m through t. The 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.

c. Army National Guard (ARNG) SIGINT Production Chain. The ARNG SIGINT IO program is managed solely within the SIGINT Production Chain. This ensures that incidents involving the compromise of SIGINT information remain within the SIGINT Production Chain under the purview of the NSA. Reference o explains in detail the requirements of the Army SIGINT Oversight Program and defines the roles and responsibilities of the various positions involved in the process. IAW reference o, ARNG SIGINT elements that conducted SIGINT activities or training exercises during the reporting period must submit a Quarterly IO Report and Commander's Signature page. ARNG SIGINT elements are not required to submit an IO Quarterly Report, of any type, if the unit did not conduct any SIGINT training during the quarter; early reporting must be pre-coordinated. 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 via email to the: Guard Technical Control and Analysis Element (G-TCAE) at <usarmy.meade.inscom.list.gtcae@mail.mil>.

d. Technical Surveillance Countermeasures (TSCM). This section applies to the NGB-J2 TSCM team, which uses electronic equipment and specialized techniques in support of the CNGB to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.

(1) Procedures. IAW approval granted by the USD(I&S) in reference u, the NGB-J2 TSCM team may conduct their activity only IAW reference e and reference v. When using TSCM equipment, the team may incidentally collect USPI without the consent of those subjected to the surveillance, provided the use meets all of the following conditions:

24 August 2022

(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.

(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 defined in reference w, such countermeasures are not targeted against the communications of any particular person or persons.

(2) Retention and Dissemination of Information Acquired During TSCM Activities.

(a) When conducting TSCM activity, the NGB-J2 TSCM team may retain or disseminate information only if it is acquired in a manner that constitutes electronic surveillance as defined in reference w to protect information from unauthorized surveillance or to enforce reference x and reference y. Any information acquired must be destroyed when no longer required for these purposes or as soon as is practicable.

(b) If the information is acquired in a manner that does not constitute electronic surveillance as defined in reference w, the information may be retained and disseminated IAW Procedures 3 and 4.

(c) The technical parameters of a communication (for example, frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes described in paragraph 5.d. above or for collection avoidance purposes. The technical parameters will be maintained IAW NG records management schedules.

6. Procedure 6: Concealed Monitoring. This procedure governs concealed monitoring of any person inside the United States or any U.S. person outside the United States for an authorized FI or CI purpose. It does not apply to concealed monitoring conducted as part of testing or training exercises when the subjects are participants who have consented to the concealed monitoring as part of an approved testing or training plan. NG intelligence and CI elements in a T32 status are not authorized to conduct concealed monitoring in the United States.

7. Procedure 7: Physical Searches. This procedure applies to nonconsensual physical searches for FI or CI purposes of any person or property in the United States and of U.S. persons or their property outside the United States.

a. Physical searches inside the United States. ARNG CI elements in a T32 status are not authorized to conduct physical searches of any person or property inside the United States.

24 August 2022

b. Physical searches outside the United States. ARNG CI activity performed outside the United States must be conducted in T10 status IAW Service policies.

8. Procedure 8: Searches of Mail and Use of Mail Covers. Procedure 8 applies to physical searches of mail, including the opening or other examination of the content of mail, in the United States and abroad for FI and CI purposes. It also applies to the use of mail covers. It does not apply to items transported by a commercial carrier (such as Federal Express or United Parcel Service). Such items are subject to the provisions of Procedure 7. ARNG CI elements in a T32 status are not authorized to search mail or to request and use mail covers. These activities must be conducted in T10 status IAW Service policies.

9. Procedure 9: Physical Surveillance. Procedure 9 applies to nonconsensual physical surveillance for FI or CI purposes. It does not apply to physical surveillance conducted as part of testing or training exercises when the subjects are participants in an exercise who have consented to the surveillance as part of an approved testing or training plan. It also does not apply to counter-surveillance, where military intelligence (MI) personnel must detect and elude foreign physical surveillance. NG MI and CI elements authorized to perform physical surveillance for FI or CI purposes may do so only while in a T10 status.

10. Procedure 10: Undisclosed Participation (UDP) in Organizations.

a. 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 participation 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 under this category of UDP.)

(2) Personal purposes.

b. NG MI and CI elements authorized to perform UDP for FI or CI purposes may do so only while in a T-10 status.

11. Procedure 11: Contracting for Goods and Services. Procedure 11 applies to contracting or other arrangements with U.S. persons for the procurement of goods and services by or for an NG intelligence component element within the United States. It does not apply to contracting with Government entities or to the enrollment of individual intelligence personnel as students with academic institutions.

a. Contracts with Academic Institutions. NG intelligence component elements may enter into contracts for goods or services with academic institutions after disclosing to appropriate institution officials the NG intelligence sponsorship. When nondisclosure of intelligence component sponsorship is necessary in contracts for enrollment of students in academic institutions, the provisions of Procedure 10 apply.

24 August 2022

b. Contracts with Commercial Organizations, Private Institutions, and Individuals.

NG intelligence component elements may contract with commercial organizations, private institutions, and individuals within the United States without revealing the sponsorship of the intelligence component only if one of the following applies:

(1) The contract is for published material available to the general public.

(2) The contract is for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, or commercial online access services (that is, an internet service provider), and incidental to approved activities.

(3) There is a written determination by the Secretary of the Army (for ARNG) or Secretary of the Air Force (for Air National Guard) that the sponsorship by an intelligence component must be concealed to protect the activities of the intelligence component concerned.

12. Procedure 12: Provision of Assistance to Law Enforcement Authorities. These provisions apply for NG intelligence component support to any Federal, State, Territorial, tribal, or local civilian law enforcement authorities.

a. Requests for NG military support to civilian law enforcement authorities. These requests are closely reviewed and processed separately for approval. Refer to Table 5 for approval authority for LEA 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 z)	Secretary of Defense (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 5. Approval Authority for LEA Support

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

(2) Intelligence-Related Activities. When the request for support to a civilian law enforcement authority involves leveraging intelligence training to meet an incidental benefit of law enforcement support, it is considered an intelligence-related activity also subject to IO and will be processed for SecDef approval IAW this procedure.

(3) Use of Federal Intelligence and Intelligence, Surveillance, and Reconnaissance (ISR) Equipment. When the request for support to a civilian LEA involves the use of Federal intelligence or ISR equipment, it will be processed for SecDef approval IAW this procedure.

b. NG intelligence component elements may provide only incidentally acquired information reasonably believed to indicate a violation of law to the appropriate LEA through 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 of this enclosure.

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

24 August 2022

d. Requests for support requiring SecDef approval under this procedure will be staffed from the Director of 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 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 website found in reference aa.

13. Procedure 13. Experimentation on Human Subjects for Intelligence Purposes. The NG intelligence component will not engage in experimentation involving human subjects for intelligence purposes.

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 bb. They must also report to their JA or IG immediately upon discovery, 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-GC, or NGB-IG channels by procedures identified in reference bb.

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 EO, Presidential directive, Intelligence Community Directive, or applicable DoD policy.

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

2. Identifying QIA. An activity is not QIA unless some connection exists between the activity and an intelligence function; only those QIAs completed as part of intelligence or intelligence-related duties, or missions are reported. Illegal or improper activities by intelligence or intelligence-related personnel in their personal capacity who have no relationship to the intelligence mission (for example, breach of discipline and simple security or ethics violations) are not subject to IO reporting and will be handled through normal disciplinary or law enforcement channels. NGB-J2, NGB-GC, or NGB-IG; the NG JFHQs-State J2, JA, or IG; or ARNG Unit Intelligence Officer (S2) or Air National Guard unit intelligence officer (IN or Director of Intelligence [Air Force (A2)]) can provide assistance in making such determinations.

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

a. Improper collection, retention, or dissemination of USPI. 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 U.S. person 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) Storing reports about USPI in intelligence files merely because the information was transmitted on a classified system.

(6) Collecting open-source USPI without a logical connection to the unit mission or correlation to a validated collection requirement.

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

b. Failure to file a proper use memorandum (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 an MI Soldier or Airman to gain access for non-MI purposes (for example, an MI traditional Guardsman accessing DoD intelligence databases to gain information for his 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 U.S. person 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 U.S. person 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 in an effort 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 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 appropriately dealt with through normal command actions, unless occurring during 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, Criminal Violations, and Federal Crimes.

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

24 August 2022

references b, c, cc, and dd. This ensures that senior DoD and Department of Justice leadership know of serious Federal crimes involving MI employees 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 either involve significant matters or are likely to receive publicity.

(2) Criminal cases 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 case related to procurement involving current or retired DoD military or civilian personnel.

(c) Any investigation into defective product(s).

(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 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 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: name, rank or civilian grade, Social Security number, military or civilian occupational specialty code, security clearance and present access, unit of assignment, employment, attachment or detail, and duties at the time of the 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 crime occurred.

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

(4) Identity of the LEA receiving the report and investigating the incident.

(5) If the report originated outside the affected command, whether or not the command submitted its own report and, if so, through what channels (for example, IO channels).

c. NGB-J2 will transmit reports received under this paragraph to the ATSD(PCLT).

d. Examples of reportable Federal crimes: 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 or threat of death or serious physical harm, unauthorized transfer of controlled technology to a foreign entity, and tampering with, or unauthorized access to, information systems.

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

(1) Reportable information collected and disseminated to NG intelligence elements by another agency, unless the intelligence component was the sole recipient.

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

(3) Crimes against property totaling \$500 or less for intelligence employees, or \$1,000 or less for other personnel.

(4) 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 AND COUNTERINTELLIGENCE DISCIPLINES AND THE NATIONAL GUARD

1. Introduction. The following intelligence and CI disciplines can be found within NG units and activities: geospatial intelligence (GEOINT), including imagery intelligence (IMINT), SIGINT, human intelligence (HUMINT), open-source intelligence (OSINT), measurements and signatures intelligence (MASINT), medical intelligence (MEDINT), and CI. These are described briefly below.
2. GEOINT and IMINT. GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on Earth. GEOINT consists of imagery, IMINT, and geospatial information which contain seven main categories: aeronautical, nautical and hydrographic, topographic and terrestrial, precise positioning and targeting, geodesy and geophysics, geographic names, and GEOINT analysis. IMINT is derived from the exploitation of collection by visual photography, infrared (IR) sensors, lasers, electro-optical sensors, and radar sensors, such as synthetic-aperture radar, wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. IMINT includes full-motion video, photographic, IR, radar, and electro-optical images captured using ground or aerial systems and other technical means. These systems may be used in support of incident awareness and assessment (IAA), consequence management, or CD activities with proper coordination under an approved mission and authority. These systems will not be used to target U.S. persons without explicit mission and authority from the SecDef. USPI gathered to save life and limb in an emergency will be purged from all NG databases when it is no longer required for dealing with the emergency. Specific policy regarding domestic imagery is addressed in Enclosure F.
3. SIGINT. SIGINT is intelligence-gathering by interception of signals, whether communications between people (communications intelligence (COMINT)) or from electronic signals not directly used in communication (electronic intelligence [ELINT]). The NSA is the only organization that can authorize SIGINT collection. Under no circumstances may units perform SIGINT collection independently or under the direction of a Governor in support of a State mission. SIGINT is heavily regulated because it involves electronic surveillance, an intrusive kind of search covered by the Fourth Amendment of reference bb. Units involved in SIGINT will be aware of and comply with applicable NSA/Central Security Service directives and policies, which include references m through t, because they dictate performance boundaries within SIGINT training and operations. ARNG exercise SIGINT must follow reference t. Exercise SIGINT (Low Level Voice Intercept, Prophet, et cetera) requires authorization from the Army Cryptologic Office through an exercise concept of operations.
4. HUMINT. HUMINT is derived from information collected and provided by human sources, both wittingly and unwittingly. HUMINT collection activities include conducting source operations; liaising with host nation officials and allied counterparts; eliciting

24 August 2022

information from select sources; debriefing U.S. and allied forces and civilian personnel, including refugees, displaced persons, third-country nationals, and local inhabitants; interrogating enemy prisoners of war and other detainees; and initially exploiting documents, media, and materiel. The manner in which HUMINT operations are conducted is dictated by both official protocol and the nature of the source of the information. NG HUMINT work generally does not involve clandestine activities. NG personnel must have a valid mission and authority to conduct any type of HUMINT activity. T32 NG units with a HUMINT mission may conduct training activities with witting participants during inactive duty for training and annual training.

5. OSINT. OSINT is collected from publicly available sources and analyzed to produce actionable intelligence. In the Intelligence Community, the term “open” refers to overt, publicly available sources. This includes media (such as newspapers, magazines, radio, and television), computer-based information (such as internet-based communities, user-generated content, social-networking sites, video-sharing sites, and blogs) and official public data or other government reports (such as budgets, demographics, hearings, legislative debates, press conferences, and public speeches). Use open-source material to collect, detect, target, or identify any U.S. persons only with proper mission, authority, and necessity. The NG has no independent authority to engage in OSINT activity.

6. MASINT. MASINT is technically derived information from sensor sets or other means not classified as SIGINT, HUMINT, or GEOINT/IMINT that results in intelligence that detects and classifies targets and identifies or describes signatures (distinctive characteristics) of a fixed or dynamic target source. Images and signals from other intelligence-gathering processes can be further examined through the MASINT discipline (for example, to determine the depth of buried objects in imagery gathered through the IMINT process). MASINT will not be used to collect, detect, target, or identify USPI without proper mission and authority. The NG has no independent authority to engage in MASINT activity.

7. MEDINT. MEDINT is the collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information used in strategic planning. It also is used in military medical planning and operations to conserve the fighting strength of friendly forces and to form assessments of foreign medical capabilities in both military and civilian sectors. NG MEDINT personnel will receive IO training IAW Enclosure D. Specific U.S. persons will not be targeted without receiving explicit mission and authority from the SecDef.

8. CI. CI involves gathering information and performing activities to protect against espionage; other intelligence activities; and sabotage or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities. T32 ARNG CI units may conduct training activity during inactive duty for training and annual training. Local LEAs must be informed if training activities occur in public areas. Role players and training targets must give prior written consent stating they knowingly are involved in a training exercise. The NG only conducts CI activities under Service or other DoD authorities and has no independent CI mission.

ENCLOSURE D

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 T32 military and civilian 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 if they are involved in intelligence or intelligence-related activities.

(4) All T32 NG units and staffs that conduct information operations, which includes cyberspace intelligence activities.

(5) TAGs and CG along with commanders, directors, IGs, and JAs or GCs of those organizations who conduct or provide advice regarding intelligence or intelligence-related activities.

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 training at least once every calendar 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 currency 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.

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 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 HUMINT missions must be trained in Procedures 6 through 10. Units with an OSINT mission must be trained on Procedure 10.
- (8) Staffs, units, or organizations that collect, process, exploit, analyze, disseminate, or retain domestic imagery, or conduct 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 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 (reference aa). The ATSD(PCLT) provides IO training resources to assist in developing unit-specific IO training at reference ee.

4. Additional Training Requirements for SIGINT Units. Commands with SIGINT elements will ensure that those elements obtain appropriate training from qualified

24 August 2022

personnel on applicable SIGINT directives. Reference e also requires training on the requirements and restrictions of references v and b with respect to the unauthorized acquisition and use of communications and information. Reference n 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 references n through r 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 E

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 local, tribal, or State 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 over, 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 equipment for SAR requires a separate PUM.

24 August 2022

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 or NGB-validated primary agency or 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, local, and tribal 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 domestic operations, 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 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. 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 ff, drug interdiction and CD activities with respect to the T32 NG mean “the use of NG personnel in drug

24 August 2022

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 ff for State CD plan support. While all State plan support is non-intelligence activity that is not subject to IO, IO training will be included in doctrinal training given to each member at initial entry and repeated annually for all personnel with an emphasis on what constitutes intelligence versus non-intelligence activities to ensure the authorities under which National Guardsmen are operating are not exceeded. See reference ff and reference gg for additional information.

(3) NG personnel providing criminal analysis support, a non-intelligence activity, to civilian LEAs under the authorities of reference ff and the approved State CD plan, will comply with reference hh and reference ii. They must also comply with the policy of the supported agency. The information under analysis is the property of the supported LEA and will not be retained in DoD or NG information systems, files, or databases, including those maintained for intelligence purposes.

(4) Any use of Federal intelligence or Federal ISR equipment for non-intelligence activity in support of the State CD mission requires separate approval. For example, the use of an MQ-9 Reaper (remotely piloted aircraft) to support the State plan requires separate approval under reference jj.

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 z. This intelligence activity is subject to IO. 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 agency and the rules under which the assignment or detail was approved.

c. IO Programs. Only NG CD programs providing intelligence support under reference y are required to maintain an IO program. State CD Coordinators, with the assistance of State IO Monitors, may use the Analysis Support Checklist located at reference aa to ensure they are not conducting unauthorized intelligence or intelligence-related activity.

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 hh and reference ii concerning the handling of information related to persons not affiliated with DoD.

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 IAW reference a and this manual.

c. While conducting operations, CRE units could incidentally or otherwise collect USPI. Upon completion of operations, all USPI must be redacted from information or files before being used in after-action reports, Mission Termination Packets, or other follow-up reports.

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 IAW this manual and reference a.

7. Cyber Intelligence. T32 NG personnel assigned to cyber intelligence and cyber ISR units and billets are subject to this manual and references a through f. This includes, but is not limited to, T32 National Guardsmen filling intelligence billets on ARNG Cyber Protection Teams and on NG Defensive Cyberspace Operations-Elements.

ENCLOSURE F

DOMESTIC IMAGERY

1. Domestic Imagery. Domestic imagery supports commander needs for operational and training requirements (such as IAA, including situational awareness and SAR). NG units may, at times, require newly collected or archived domestic imagery. Collecting imagery inside the United States 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 U.S. persons and private property. Individuals may be held personally responsible for any violation of law or inappropriate use of domestic imagery.

b. Missions. IAW reference kk, 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 Secretary of Defense.

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 domestic imagery from national satellites. IAW references ll and 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 U.S. person is not considered USPI.

3. Domestic Imagery from Airborne Platforms. Follow policy of the gaining CCMD, 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 by the T32 NG for intelligence-related or IAA purposes.
- d. Refer to Table 6 for help in determining whether a PUM or DILR is required.

Type of Asset	Type of Activity	Required Document
Intelligence Component Capability (for example, JSTARS, MC-12, MQ-9, RQ-7, or RQ-11)	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, RC-26, 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, JSTARS, MC-12, MQ-9, RQ-7, or RQ-11)	T32 Intelligence-related activity (for example, ISR training)	PUM
Non-Intelligence Component Capability (for example, A-10, F-15, F-16, RC-26, 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, JSTARS, MC-12, MQ-9, RQ-7, or RQ-11)	Non-intelligence activity (for example, IAA)	PUM
Non-Intelligence Component Capability (for example, A-10, F-15, F-16, RC-26, UH-60, or UH-72)	Non-intelligence activity (for example, IAA)	DILR

Table 6. Domestic Imagery Collection Documentation

4. CD PUMs. PUMs and DILRs are not required for domestic imagery collection missions flown in support of an LEA 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 equipment, unmanned aircraft system, or remotely piloted aircraft (such as the MC-12, JSTARS, MQ-9, RQ-7, or RQ-11).

b. The analysis of the images collected is done by members on CD-funded orders 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 and RC-26 sensors for other purposes, such as IAA, likely requires a PUM or DILR. All PUMs or DILRs must be filed IAW paragraph 6 below.

5. Domestic Imagery from Commercial Satellites.

a. NG intelligence component elements may obtain archived National Geospatial-Intelligence Agency domestic commercial satellite imagery (for example, the Net-Centric Geospatial Intelligence Discovery Services) without higher-level approval 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 (DSCA) in either T10 or T32 status. NG intelligence component elements may also use domestic open-source, publicly available, and other commercial imagery (for example, U.S. Geological Survey imagery, Google Earth™ imagery, and Falcon View™ imagery). The obligation of compliance with IO and other policies is on 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 is provided in Figure 8. The NG intelligence component element may only collect, process and exploit, analyze, assess, or disseminate commercial imagery or imagery-associated products in support of their approved mission.

Print on State letterhead

[Insert Date]

Subject: *[INSERT YEAR and UNIT (for example, NGB-J2 2021)] Commercial Domestic Imagery and Other Geospatial Information Use Authorization*

1. (CUI) In accordance with Chief of the National Guard Bureau Manual 2000.01B, "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 the following: *INSERT SPECIFIC DATABASES AND SYSTEMS USED BY THE UNIT [for example, ArcGIS, Defense Collaboration Services, Falcon View™, 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, however, other local, State and Federal agencies may request support from time to time. The imagery and information may be disseminated via hard or softcopy methods that include shared enterprise portals such as National Guard Bureau- Joint Intelligence Directorate SharePoint, Guard Knowledge Online, 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."
5. (U) My point of contact is *[name, contact number, email]*.

Figure 8. Internal MFR Certifying Proper Use of Commercial Domestic Imagery

24 August 2022

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

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 could be collected of a private structure so that the imagery can be used as a visual navigational aid or to simulate targeting during training. However, imagery may not be collected to gather any specific information about a U.S. person or private entity, without consent, nor may stored imagery be retrievable by reference to a U.S. person'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 U.S. persons without consent, unless expressly approved by the SecDef, IAW U.S. law and regulations. Civilian LEAs, such as U.S. Customs and Border Protection, the Federal Bureau of Investigations, 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 to prepare crews to conduct missions in deployed locations, including the ability to track mobile objects in both urban and rural settings. NG personnel are not authorized to record or retain data acquired during these training missions, nor will this data be disseminated in any form, unless otherwise required by law or policy, subject to explicit NGB-J2 approval. 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 appropriate activities of this nature are supported by an applicable PUM that addresses the activity in detail as prescribed in this enclosure.

(2) Proper approval authority and other applicable permissions (that is, Federal Aviation Administration approval for unmanned aircraft systems and remotely piloted aircraft airspace) 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 U.S. person or the person's identifiably unique features. The "targets" captured during these visual reconnaissance training activities are not recorded or retained on weapon system platform or off-board media.

24 August 2022

(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 in general.

d. The use of NG unmanned aircraft systems and remotely piloted aircraft must comply with the policy in references jj and mm.

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

a. For the PUM and DILR.

(1) PUMs and DILRs do not constitute the approval authority for the underlying T-32 training, exercise, or operation.

(2) PUMs and DILRs are an entity's notice of collection, 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 U.S. person, 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 in the rank of Major or above, 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 QIA, reportable IAW procedures established in reference bb.

(4) Any NG JFHQs-State that owns or has operational control over NG assets that conduct domestic imagery activities as defined in paragraph 1.b. above is responsible for creating 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 CCMD 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.

24 August 2022

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

(a) Routine training and DoD exercises, excluding DSCA and IAA exercises, in routine training areas. DSCA, IAA, and State exercises require separate PUMs or DILRs. For example, IAA missions in support of ARDENT SENTRY and VIGILANT GUARD exercises as well as State wildfire response exercises require separate PUMs, whereas RED FLAG and ANGEL THUNDER exercises do not.

(b) SAR missions.

(c) TAG's or CG's IAA requirements.

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

(a) Subject Line. Identify the document as an NG T32 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 protection of non-DoD affiliated person information and domestic imagery policy documents.

(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 MASINT will be collected or disseminated (include authorities if any SIGINT, HUMINT, or MASINT will be collected).

(d) Paragraph 3. U.S. Person or Non-DoD Affiliated Person statement. Include either:

1. The following statement: "No U.S. persons (PUMs) or Non-DoD Affiliated Persons will be targeted during these missions. Any personally identifying information unintentionally and incidentally collected about specific U.S. persons will be purged and destroyed unless it may be lawfully retained and disseminated to other governmental agencies that have a need for it IAW applicable laws, regulations, and policies."

2. If a U.S. person (PUM) or non-DoD-affiliated person (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, including, reference II. 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

24 August 2022

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 protection of non-DoD affiliated person information 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.

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

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

(f) Paragraph 5. Judge Advocate review. Include the following: "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, Vermont National Guard) Office of the Staff Judge Advocate with [JA contact information] for compliance with law, policy, and intelligence oversight."

(g) Paragraph 6. Proper Use statement and certification by NG JFHQ-State J2. This must be a field-grade officer in the rank of Major or above, or the civilian equivalent. If the NG JFHQs-State J2 does not meet the rank requirement, a field-grade officer in the rank of Major or above in the J2's chain of command 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 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."

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 NG JFHQs-State J2 point of contact and his or her contact information—This must be field-grade officer in the rank of Major or above or the civilian equivalent.

(h) Paragraph 7. Point of contact information. Name, office, telephone number, and email address or fax number for the PUM or DILR point of contact.

(i) Signature authority. The signature of the certifying official (must be a field-grade officer in the rank of Major or above, or civilian equivalent). If the NG JFHQs-

24 August 2022

State J2 does not meet the rank requirements, a field-grade officer in the J2's chain of command is authorized to sign.

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

(a) Approval resides with NGB-J2.

(b) Requests will be submitted via email to NGB-J2 at <ng.ncr.arng.list.ngb-j2-intel-oversight@mail.mil> or fax 703-601-2263. PUMs 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 CG may authorize airborne domestic imagery collection, including the lawful acquisition of USPI when that support is consistent with reference k 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 U.S. Northern Command and/or U.S. Indo-Pacific Command 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 domestic imagery. The intelligence organization's certifying official signs 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 8, or the NGB-J2 IO website, reference aa 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 aa 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.

24 August 2022

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 (DAART), Intelink or the Secret Internet Protocol Router Network [SIPRNET]) 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 preclude analysis or exploitation, if applicable, of imagery of a sensitive Federal named area of interest.

e. IAW reference nn and reference oo, 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 domestic operations, including IAA, can be intense and immediate. Personnel will refer all media inquiries and other requests for information, including imagery, from outside of 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 general 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 depict disaster areas and disaster response activities.

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

ENCLOSURE G

INTELLIGENCE SUPPORT TO FORCE PROTECTION

1. General. NG intelligence component support to force protection (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 U.S. persons) 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. As a general rule, 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 regulation but must comply with reference hh and reference ii.

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

c. LEAs 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 Enclosure B). Follow retention and dissemination rules in Procedures 3 and 4 in Enclosure B. 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, 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

24 August 2022

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

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 Guardsmen 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 non-commissioned 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 (see Enclosure B). 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 Investigations, 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 H

THE INTERNET AND PUBLICLY AVAILABLE INFORMATION

1. General.

a. NG intelligence component elements must have official mission requirements before collecting, using, retaining, or disseminating even publicly available information about U.S. persons. IAW Procedure 10, 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, intelligence and CI personnel must understand how to analyze and characterize IP addresses, Uniform Resource Locators (URLs), and email addresses IAW reference pp.

2. IP Addresses. Similar to a telephone number, the numeric string composing an IP address does not, without further information, identify or consist of information about a U.S. person. However, open-source information about IP addresses is available on the World Wide Web. Sometimes, the information is general and does not allow one to determine whether the IP address constitutes information about a U.S. person. In other instances, the available information is specific and does allow such a determination. NG intelligence and CI components are not required to try to decipher an IP address as soon as they encounter one. They are only required to engage in such an inquiry once a decision is made to conduct analysis that is focused on specific IP addresses. Prior to such analysis, IP addresses may be treated as "data acquired by electronic means." Such data is not considered to be collected until it has been processed into intelligible form. There are no IO restrictions on the maintenance or disposition of information that is not considered to have been "collected."

a. Once the decision is made to analyze specific IP addresses, the "collecting" component is obligated to conduct a reasonable and diligent inquiry to determine whether any of the IP addresses are associated with U.S. persons. If the NG intelligence component still cannot reasonably determine whether a given IP address is associated with a U.S. person, then it may presume that unattributed IP addresses do not constitute information about a person, and the IP address may be the subject of inquiry without regard to whether it is associated with a U.S. person. However, if the NG intelligence component subsequently obtains information indicating that an IP address is associated with a U.S. person, then the presumption is overcome and that IP address must be handled IAW the procedures governing the collection of information about U.S. persons. An inquiry revealing that an IP address is assigned to a U.S. service provider is not necessarily sufficient information to presume that the address is associated with a U.S. person. In the sense that a telephone number gives more information about the caller than about the phone company, the IP address gives more information about the individual connection than about the service provider that is facilitating that connection.

24 August 2022

b. Some Internet service providers principally serve a U.S.-based clientele. An IP address within a block assigned to such an Internet service provider might merit the presumption that any IP address within that block identifies a U.S. person. Conversely, if a group of IP addresses is known to be assigned to a non-U.S. person (for example, a foreign corporation), then the NG intelligence component may presume that any given IP address within that block is associated with a non-U.S. person. The collecting component should document the efforts made to determine whether the IP address in question is associated with a U.S. person.

3. Email Addresses. Email addresses, unlike both IP addresses and URLs, are nearly universally associated with individuals. 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 U.S. person. Sometimes, the name to the left of the “@” will provide persuasive evidence that the email address is associated with a U.S. person; for example, the person may be a well-known public figure 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 U.S. person. Some service providers predominately serve a non-U.S.-based clientele, and email accounts with such providers may be presumed not to be U.S. persons’ accounts. Other service providers are so closely affiliated with the United States that any email account with that provider should be presumed to be associated with a U.S. person (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 pp.

b. All other email addresses may be treated similar to the approach described for the treatment of IP addresses. Email addresses that are not self-evidently associated with U.S. persons may be acquired, retained, and processed by NG intelligence component elements with the appropriate mission and authority without making an effort to determine whether any given address is associated with a U.S. person so long as the component does not engage in analysis focused upon specific addresses. Once such analysis starts, the NG intelligence component must make an effort to determine whether the addresses are associated with U.S. persons. Unlike IP addresses, there is no central repository of email addresses to assist the component in identifying them. Instead, the component must rely on traditional methods to try to determine whether a given address is being used by a U.S. person.

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

24 August 2022

4. URL. In determining whether a URL identifies a U.S. person, 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-U.S. person. Conversely, if the domain is associated with the U.S. (for example, .gov, .mil), then the URL should be presumed to be information that identifies a U.S. person. Several domains are universally available, such as .com, .net, and .org, and do not provide information about whether the URL identifies a U.S. 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 U.S. person. As with all information, when the URL name is obtained to show that the URL is associated with a U.S. person, then the collection, retention, and dissemination of the URL name must be handled IAW IO procedures.

a. Unlike IP and e-mail addresses, URLs are, almost by definition, publicly available. Therefore, even if they identify U.S. persons, lists of URLs may be maintained by NG intelligence component elements provided they are within the scope of an authorized intelligence 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 element wants to collect information beyond what is available on the website, then it must make an effort to determine whether the person about whom it is collecting is a U.S. person and, if so, comply with IO procedures.

5. Social Media Use.

a. National Guardsmen who have been appropriately assigned to support IAA, SAR, or other domestic operations may monitor social media, including DATAMNR™ and other approved 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 kept for the duration of the domestic operations to aid SAR. In this circumstance, consent is implied under the assumption that the individual wants to be rescued. All personally identifiable information must be destroyed immediately following the conclusion of domestic operations. DoD DATAMNR™ First-Alert accounts may be used by Guardsmen with .mil email addresses in a T32 or a T10 duty status to support authorized DoD missions.

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

ENCLOSURE I

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 qq. At a minimum, the binder will contain:
 - a. Appointment letters for primary and alternate 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. Use Service-specific systems of record management for maintaining IO training records (that is, Digital Tracking and Management System [DTMS] for ARNG units), but also ensure that IO Monitors can access and validate completeness of training records.
 - e. Copies of references a through i and bb, this manual, and the State IO standard operating procedure or policy.
 - f. Staff/Unit/Organization-oriented IO Self-Inspection Checklist. This is created by using the applicable checklists in Enclosure J.
 - g. Self-inspection and inspection records to be maintained for three years.
 - h. QIA, S/HSM, and Federal crime reporting processes and report formats.
 - i. Copies of any QIA, S/HSM, and Federal crime reports to be maintained for three years.
 - j. Annual file review certification MFR to be maintained for three years.

ENCLOSURE J

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 legality and propriety. Inspectors may review IO programs, which include IO Monitor appointment letters, State IO policy, training records, training materials, IO Continuity Binders, and the mandatory reference documents (references a through i and reference bb). 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 aware of basic IO requirements (for example, what constitutes a U.S. person; 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. The NGB IG IO Branch will use reference bb for inspecting NG JFHQs-State and unit T-32 IO programs.

3. DoD SIOO inspection checklists and other inspection information are available in reference c and on their websites in reference ee and reference rr.

4. 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 J

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, Service, and National Guard policy? (See reference a, Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, paragraph 4, and Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, 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? (2000.01B, 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? (2000.01B, Enclosure A, paragraph 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? (2000.01B, Enclosure A, paragraph 1.c.(1)(b))	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? (2000.01B, Enclosure A, paragraph 1.c.(1)(a))	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? (2000.01B, Enclosure A, paragraph 1.c.(2)(a))	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? (2000.01B, Enclosure A, paragraph 1.c.(2)(b))	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 this manual? (2000.01B, Enclosure A, paragraph 1.c.(2)(a))	Yes or No

Table 7. Procedure 1 Self-Inspection Checklist

APPENDIX B TO ENCLOSURE J

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 the performance of an authorized intelligence mission or function assigned to you in the appropriate duty status? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 2.a.)	Yes or No
2. Does all U.S. person information (USPI) that you collect fall into a category specified in CNGBM 2000.01B Enclosure A, paragraphs 2.a(1) through (13)?	Yes or No
3. Do you address circumstances where an entity or individual is voluntarily providing on a recurring basis USPI that is not relevant to an authorized mission or function? (See CNGBM 2000.01B Enclosure A, paragraph 2.b(3))	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? (See CNGBM 2000.01B Enclosure A, paragraph 2.d(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? (See CNGBM 2000.01B Enclosure A, paragraph 2.d(3))	Yes or No
6. Do you have a process to ensure that collection of authorized USPI is performed in accordance with this procedure? (See CNGBM 2000.01B Enclosure A, paragraph 2.e.)	Yes or No

Table 8. Procedure 2 Self-Inspection Checklist

APPENDIX C TO ENCLOSURE J

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? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 3)	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? (CNGBM 2000.01B, Enclosure A, paragraph 3)	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.g.)	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.e.)	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 CNGBM 2000.01B, 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 9. 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. (CNGBM 2000.01B, Enclosure A, paragraph 3.i.)	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.j.(1))	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.j.(2)(a))	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.j.(2)(b))	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.j.(2)(c))	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.k.)	Yes or No
11. Do you review all electronic and hardcopy files at a minimum of 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? (CNGBM 2000.01B, Enclosure A, paragraph 3.l.)	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? (CNGBM 2000.01B, Enclosure A, paragraph 3.l.)	Yes or No

Table 9, continued. Procedure 3 Self-Inspection Checklist

APPENDIX D TO ENCLOSURE J

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? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 4)	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? (CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4))	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? (CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(b)-(f))	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 CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(b)?	Yes or No
6. Have you disseminated USPI to other Department of Defense elements?	Yes or No (If No, proceed to question 8.)
7. If you have disseminated USPI to other Department of Defense elements, has the dissemination met the requirements in CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(c)?	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 CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(d)?	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 CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(e)?	Yes or No

Table 10. 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 Enclosure A, paragraph 4.a.(4)(f)?	Yes or No
13. Have you disseminated USPI to any 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 CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(g)?	Yes or No
15. Have you disseminated USPI to a 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 CNGBM 2000.01B, Enclosure A, paragraph 4.a.(4)(h)?	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 delegate approve, after notifying the Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency, the dissemination? (CNGBM 2000.01B, Enclosure A, paragraph 4.b.)	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? (CNGBM 2000.01B, Enclosure A, paragraph 4.f.)	Yes or No
19. Has any dissemination of USPI not conformed to the conditions set forth in Procedure 4 of CNGBM 2000.01B? If Yes, has the Defense Intelligence Component Head approved the dissemination? (CNGBM 2000.01B, Enclosure A, paragraph 4.c.)	Yes or No

Table 10, continued. Procedure 4 Self-Inspection Checklist

APPENDIX E TO ENCLOSURE J

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? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 5.a.)	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)? (CNGBM 2000.01B, Enclosure A, paragraph 5.b.)	Yes or No
3. Are all requests to perform electronic surveillance, which includes 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? (CNGBM 2000.01B, Enclosure A, paragraph 5.c.)	Yes or No
4. Do you ensure that SIGINT cryptologic element activities are conducted in accordance with applicable USSIDs? (CNGBM 2000.01B, Enclosure A, paragraph 5.d.)	Yes or No
5. National Guard Bureau Joint Intelligence Directorate (NGB-J2) Technical Surveillance Countermeasures (TSCM) Team only: Do you conduct all activity in accordance with Department of Defense Manuals S-5240.05 and 5240.01? (CNGBM 2000.01B, Enclosure A, paragraph 5.e.(1))	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 of the following conditions: <ul style="list-style-type: none"> 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 11. Procedure 5 Self-Inspection Checklist

<p>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.</p> <p>d. If the use of TSCM constitutes electronic surveillance as that term is defined in the Foreign Intelligence Surveillance Act (FISA), such countermeasures are not targeted against the communications of any particular person or persons. (CNGBM 2000.01B, Enclosure A, paragraph 5.e.(1))</p>	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 FISA to protect information from unauthorized surveillance or to enforce Chapter 119 of Title 18 and Section 605 of Title 47 U.S. Code? (CNGBM 2000.01B, Enclosure A, paragraph 5.e.(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? (CNGBM 2000.01B, Enclosure A, paragraph 5.e.(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 FISA, do you retain and disseminate that USPI in accordance with Procedures 3 and 4? (CNGBM 2000.01B, Enclosure A, paragraph 5.e.(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 CNGBM 2000.01B, Enclosure A, paragraph 5.e.(2)(c)?	Yes or No

Table 11, continued. Procedure 5 Self-Inspection Checklist

APPENDIX F TO ENCLOSURE J

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? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 6.b.)	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)? (CNGBM 2000.01B, Enclosure A, paragraph 6.c.)	Yes or No
3. Are NG intelligence component personnel who are authorized to conduct or approve concealed monitoring trained and certified? (Department of Defense Manual 5240.01, paragraph 3.6)	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"? (Department of Defense Manual 5240.01, paragraph 3.6.b.)	Yes or No

Table 12. 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? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 7.b.)	Yes or No

Table 13. 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? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 8.c.)	Yes or No

Table 14. 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? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 9.b.)	Yes or No

Table 15. 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? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 10.b.)	Yes or No

Table 16. Procedure 10 Self-Inspection Checklist

Inspection Item	Yes or No
Do National Guard intelligence component elements enter into contracts for goods or services only in accordance with Procedure 11? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 11)	Yes or No

Table 17. Procedure 11 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)? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph 12.a.)	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? (CNGBM 2000.01B, Enclosure A, paragraph 12.c.)	Yes or No
3. Do NG intelligence elements providing analysis support to a civilian LEA under Title 10 U.S. Code §284 authorities comply with the privacy rules governing the agency and the rules under which the assignment or detail was approved? (CNGBM 2000.01B, Enclosure E, paragraph 4.B.)	Yes or No
4. Is all information being analyzed by NG intelligence elements providing analysis support to civilian LEAs under the approved State counterdrug plan retained in LEA files and databases and not in Department of Defense or NG intelligence files or databases? (CNGBM 2000.01B, Enclosure A, paragraph 12.d.)	Yes or No

Table 18. Procedure 12 Self-Inspection Checklist

Inspection Item	Yes or No
1. Do National Guard intelligence component elements engage in experimentation involving human subjects for intelligence purposes? (Chief of the National Guard Bureau Manual 2000.01B, Enclosure A, paragraph 13)	Yes or No

Table 19. Procedure 13 Self-Inspection Checklist

APPENDIX G TO ENCLOSURE J

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? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure A, paragraph a and Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, paragraph 4.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? (CNGBI 2000.01D, paragraph 4.b.)	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? (CNGBI 2000.01D, paragraph 4.d.)	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 (CHATS) or Counterintelligence/Human Intelligence Information Management System (CHIMS), or resources intended for CI and HUMINT activities, unless authorized by the Secretary of Defense or designee? (CNGBI 2000.01D, paragraph 4.d.)	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? (CNGBI 2000.01D, paragraph 4.f.)	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? (CNGBM 2000.01B, Enclosure A, paragraph b.)	Yes or No
7. Is training documented and the documentation retained for three years? (CNGBM 2000.01B, Enclosure I, paragraph 2)	Yes or No
8. Have employees of NG intelligence component elements received annual intelligence oversight training tailored to the unit, staff, or organization's mission? (CNGBM 2000.01B, Enclosure A, paragraph b.)	Yes or No

Table 20. Employee Conduct Self-Inspection Checklist

9. Is training documented and the documentation retained for three years?	Yes or No
10. Do all employees of NG intelligence component elements carry out reporting responsibilities as described in Enclosure B? (CNGBM 2000.01B)	Yes or No

Table 20, continued. Employee Conduct Self-Inspection Checklist

APPENDIX H TO ENCLOSURE J

NATIONAL GUARD JOINT FORCE HEADQUARTERS-STATE J2 SELF-INSPECTION
CHECKLIST

Inspection Item	Yes or No
1. Is the National Guard (NG) Joint Force Headquarters–State (NG JFHQs-State) Joint Intelligence Directorate (J2) knowledgeable of all State intelligence and intelligence-related activities carried out in the State? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, Enclosure A, paragraph 14.a.)	Yes or No
2. Has the J2 identified all intelligence staffs, units, and personnel performing intelligence and intelligence-related functions within the State and verified compliance with appropriate directives? (CNGBI 2000.01D, Enclosure A, paragraph 14.h.)	Yes or No
3. Has the J2 established and maintained an effective intelligence oversight (IO) Program for all personnel assigned or attached to the NG JFHQs-State J2? (CNGBI 2000.01D, Enclosure A, paragraph 14.d.)	Yes or No
4. Have experienced intelligence professionals been appointed in writing to serve as NG JFHQs-State primary and alternate IO Monitors? (CNGBI 2000.01D, Enclosure A, paragraph 14.e.)	Yes or No
5. Are copies of the signed appointment memos posted in the NG JFHQs-State J2 workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01D, Enclosure A, paragraph 14.e.)	Yes or No
6. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.f.)	Yes or No
7. Are all NG JFHQs-State intelligence component personnel and JA and IG personnel with IO responsibilities familiar with IO statutory and regulatory guidance, including reporting responsibilities and all restrictions? (CNGBI 2000.01D, Enclosure A, paragraph 14.f.)	Yes or No
8. Is IO training documented and is the documentation retained for three years?	Yes or No
9. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.g.)	Yes or No

Table 21. NG JFHQs-State J2 Self-Inspection Checklist

10. Is this training documented and is the documentation retained for three years?	Yes or No
11. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.k.)	Yes or No
12. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.l.)	Yes or No
13. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.m.)	Yes or No
14. 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? (CNGBI 2000.01D, Enclosure A, paragraph 14.n.)	Yes or No

Table 21, continued. NG JFHQs-State J2 Self-Inspection Checklist

APPENDIX I TO ENCLOSURE J

NATIONAL GUARD COMMANDER, DIRECTOR, AND 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? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, Enclosure A, paragraph 17.b.)	Yes or No
2. Has the Commander, Director, or SIO received initial and annual IO training? (CNGBI 2000.01D, Enclosure A, paragraph 17.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? (CNGBI 2000.01D, Enclosure A, paragraph 17.e.)	Yes or No
4. Has the Commander, Director, or SIO established and maintained an effective IO program for all personnel assigned or attached to the National Guard Joint Force Headquarters–State (NG JFHQs–State) Joint Intelligence Directorate? (CNGBI 2000.01D, Enclosure A, paragraph 17.c.)	Yes or No
5. Has the Commander, Director, or SIO appointed in writing experienced intelligence professionals to serve as NG JFHQs–State primary and alternate IO Monitors? (CNGBI 2000.01D, Enclosure A, paragraph 17.d.)	Yes or No
6. Are copies of the signed appointment memos posted in the workspaces and filed in the IO Continuity Binder? (CNGBI 2000.01D, Enclosure A, paragraph 17.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 (USPI) are trained annually on the civil liberties and privacy protections that apply to such information? (CNGBI 2000.01D, Enclosure A, paragraph 17.f.)	Yes or No

Table 22. 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 JA for review and submission to the Office of the National Guard Bureau General Counsel if required? (CNGBI 2000.01D, Enclosure A, paragraph 17.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? (CNGBI 2000.01D, Enclosure A, paragraph 17.h.)	Yes or No
10. Has the Commander, Director, or SIO imposed appropriate sanctions upon any employees who violate the provisions of CNGBI 2000.01 or other applicable policies? (CNGBI 2000.01D, Enclosure A, paragraph 17.g.)	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 USPI 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? (CNGBI 2000.01D, Enclosure A, paragraph 17.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? (CNGBI 2000.01D, Enclosure A, paragraph 17.k.)	Yes or No
13. Has the Commander, Director, or SIO submitted a quarterly IO report to the State Joint Intelligence Directorate? (CNGBI 2000.01D, Enclosure A, paragraph 17.l.)	Yes or No

Table 22, continued. NG Commander, Director, and Senior Intelligence Officer of Intelligence or Intelligence-Related Activity Organizations Self-Inspection Checklist

APPENDIX J TO ENCLOSURE J

NATIONAL GUARD INTELLIGENCE OVERSIGHT MONITOR
SELF-INSPECTION CHECKLIST

Inspection Item	Yes or No
1. Has the IO Monitor received initial and annual IO training? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, Enclosure A, paragraph 18.a.)	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? (CNGBI 2000.01D, Enclosure A, paragraph 18.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 (IAW) Chief of the National Guard Bureau Manual [CNGBM] 2000.01B, Enclosure D? (CNGBI 2000.01D, Enclosure A, paragraph 18.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? (CNGBI 2000.01D, Enclosure A, paragraph 18.c)	Yes or No
5. Has the IO Monitor maintained an IO Continuity Binder in accordance with CNGBM 2000.01B, Enclosure I? (CNGBI 2000.01D, Enclosure A, paragraph 18.d.)	Yes or No
6. Has the IO Monitor maintained copies of State IO policy and applicable references so they are available to the organization? (CNGBI 2000.01D, Enclosure A, paragraph 18.d.)	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 IG from the DoD Senior Intelligence Oversight Official, major command, or National Guard Bureau? (CNGBI 2000.01D, Enclosure A, paragraph 18.f.)	Yes or No

Table 23. 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? (CNGBI 2000.01D, Enclosure A, paragraph 18.g.)	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? (CNGBI 2000.01D, Enclosure A, paragraph 18.h.)	Yes or No
10. Has the IO Monitor immediately routed questionable intelligence activity reports and reports of incidents or significant or highly sensitive matter as specified in CNGBI 2000.01D, Enclosure A, paragraph 18.g.?	Yes or No
11. Has the IO Monitor submitted a quarterly IO report through the chain of command to the State IG? If you are an Air National Guard unit IO Monitor, have you provided a copy to the gaining major command, if required? (CNGBI 2000.01D, Enclosure A, paragraph 18.j.)	Yes or No

Table 23, continued. NG Intelligence Oversight Monitor Self-Inspection Checklist

APPENDIX K TO ENCLOSURE J

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? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01D, Enclosure A, paragraph 19.a.)	Yes or No
2. Are personnel familiar with the policies contained in CNGBI 2000.01D; Procedures 1-4 and 12; 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? (CNGBI 2000.01D, Enclosure A, paragraph 19.b.)	Yes or No
3. Do personnel conduct intelligence and intelligence-related activities in accordance with applicable law and policy, including CNGBI 2000.01D and Manual 2000.01C and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGBI 2000.01D, Enclosure A, paragraph 19.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? (CNGBI 2000.01D, Enclosure A, paragraph 19.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? (CNGBI 2000.01D, Enclosure A, paragraph 19.e.)	Yes or No
6. Are personnel able to identify the organization's IO Monitor and do they know how to establish contact? (CNGBI 2000.01D, Enclosure A, paragraph 19.f.)	Yes or No

Table 24. NG Intelligence Component Personnel Self-Inspection Checklist

ENCLOSURE K 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 Enclosure A, paragraph 2.b of this manual.
2. Special collection techniques require additional approval. The flowchart in Figure 9 represents the decision-making process when considering how to handle USPI when conducting NG intelligence and intelligence-related missions and functions.

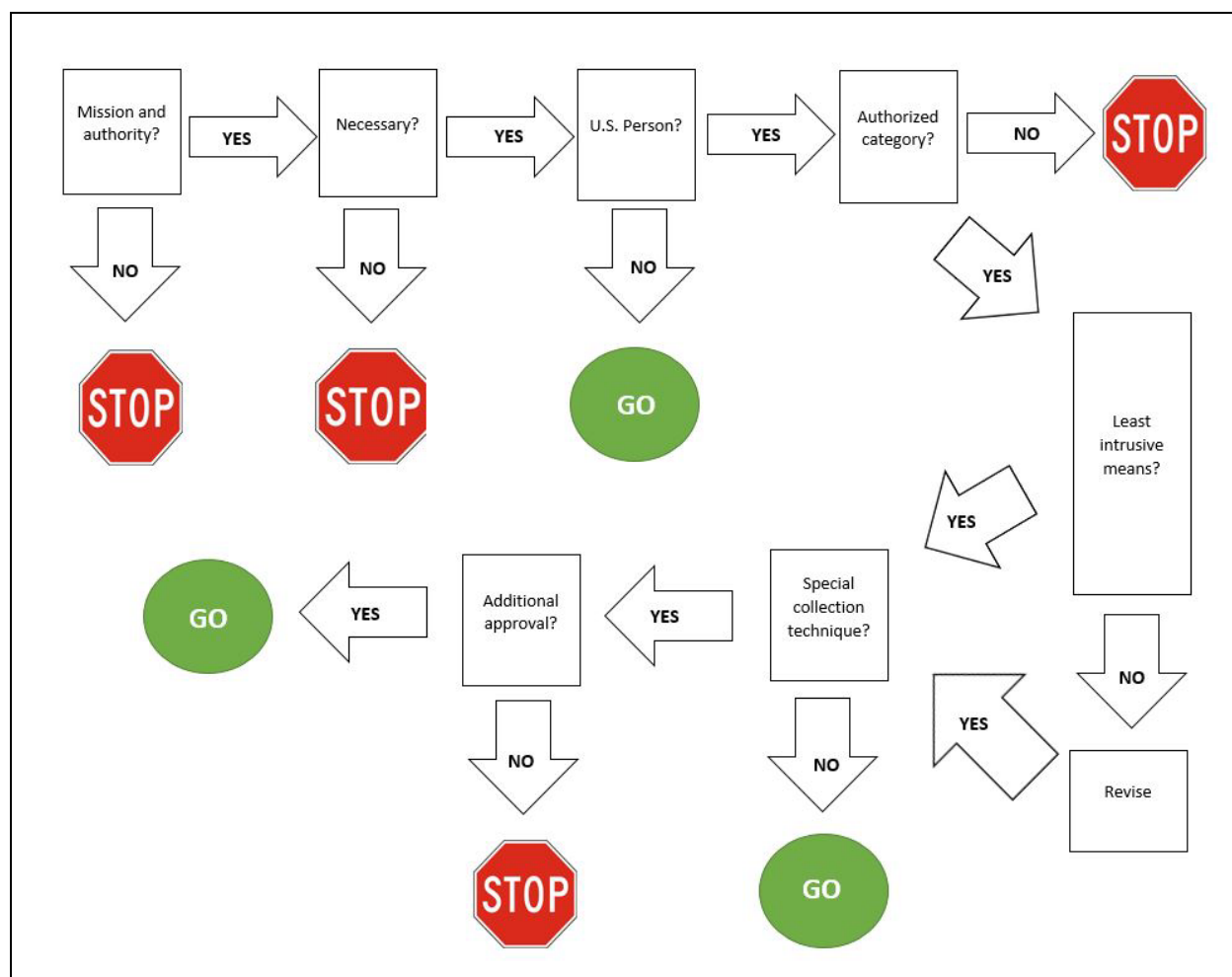


Figure 9. The Intelligence Oversight Process

3. Steps in working through the Intelligence Oversight Process are as follows.
 - 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,

24 August 2022

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 (Procedure 11), 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 L

REFERENCES

PART I. REQUIRED

- a. Chief of the National Guard Bureau (CNGB) Instruction 2000.01D, 18 January 2022, "National Guard Intelligence Activities"
- 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 August 2007, "DoD Intelligence Activities," Incorporating Change 3, 09 November 2020
- e. DoD Manual 5240.01, 08 August 2016, "Procedures Governing the Conduct of DoD Intelligence Activities"
- f. DoD 5240.1-R, 07 December 1982, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," Incorporating Change 2, 26 April 2017
- g. Army Regulation 381-10, 03 May 2007, "U.S. Army Intelligence Activities"
- h. Department of the Army Memorandum, 15 August 2016, "Implementing Guidance for Intelligence Oversight"
- i. Air Force Instruction 14-404, 03 September 2019, "Oversight of Intelligence Activities"
- j. CNGB Instruction 5000.01B, 24 January 2020, "Chief of the National Guard Bureau Issuances Program"
- k. Constitution of the United States of America, 04 March 1789, Amended 07 May 1992
- l. Presidential Policy Directive 28, 17 January 2014, "Signals Intelligence Activities"
- m. United States Signals Intelligence Directives (USSID) SP0018 (S), 27 July 2003
- n. USSID SE1000 (Army), 11 May 2012 (U)
- o. USSID 1000 ANNEX A (U//FOUO), 20 September 2016

- p. USSID SE1600NG (ARNG) (S), 22 March 1993
- q. USSID 3000 (Air Force) (U//FOUO), 17 October 2019
- r. USSID SE 3500 (ANG) (S), 11 January 2013
- s. USSID 3775 (ANG) (U//FOUO), 16 April 2015
- t. USSID 1221, Exercise SIGINT (S), 20 August 2018, Revised 18 January 2019
- u. 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)"
- v. DoD Manual S-5240.05, 23 April 2015, "(U) The Conduct of Technical Surveillance Countermeasures (TSCM)," Incorporating Change 2, 04 March 2017
- w. Title 50 United States Code (U.S.C.), Chapter 36, "The Foreign Intelligence Surveillance Act (FISA)"
- x. 18 U.S.C. Chapter 119, "Wire and Electronic Communications Interception and Interception of Oral Communications"
- y. 47 U.S.C. Section 605, "Unauthorized Publication or Use of Communications"
- z. 10 U.S.C. Section 284, "Support for Counter-drug Activities and Activities to Counter Transnational Organized Crime"
- aa. National Guard Bureau Joint Intelligence Directorate (NGB-J2) NIPRNET Intelligence Oversight Program website: <https://gko.portal.ng.mil/joint/j2/J23/NG-J2_IO/default.aspx>, accessed 21 July 2022
- bb. CNGB Instruction 0700.01A, 21 December 2018, "Inspector General Intelligence Oversight"
- cc. Memorandum of Understanding Between the Attorney General and the Secretary of Defense, August 1995, "Reporting of Information Concerning Federal Crimes"
- dd. DoD Instruction 5240.04, 01 April 2016, "Counterintelligence (CI) Investigations," Incorporating Change 2, 18 September 2020
- ee. DoD Senior Intelligence Oversight Official NIPRNET website: <<https://dodsioo.defense.gov/>>, accessed 21 July 2022
- ff. 32 U.S.C. Section 112, "Drug Interdiction and Counter-drug Activities"
- gg. CNGB Instruction 3100.01B, 06 March 2020, "National Guard Counterdrug Support Program"

- hh. DoD Directive 5200.27, 07 January 1980, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"
- ii. CNGB Instruction 2400.001A, 07 November 2013, "Acquisition and Storage of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," Validity Extended to 01 March 2021
- jj. Secretary of Defense Policy Memorandum, 18 August 2018, "Guidance for the Domestic Use of Unmanned Aircraft Systems in U.S. National Airspace"
- kk. NGA Instruction 8900.5, 02 January 2020, "Domestic Imagery," Incorporating administrative update, 09 March 2020
- ll. NGA Instruction 1806, 15 March 2019 , "Domestic Imagery," Incorporating administrative update, 15 January 2020
- mm. CNGB Instruction 7500.00, 13 October 2016, "Domestic Use of National Guard Unmanned Aircraft Systems"
- nn. DoD Instruction 8170.01, 02 January 2019, "Online Information Management and Electronic Messaging," Incorporating Change 1, Effective 24 August 2021
- oo. Deputy Secretary of Defense Memorandum, 16 January 2018, "Conducting Official Business on Electronic Messaging Accounts"
- pp. DoD Office of General Counsel Memorandum, 06 February 2001, "Principles Governing the Collection of Internet Addresses by DoD Intelligence and Counterintelligence Components"
- qq. CNGB Instruction 5001.01, 05 December 2016, "National Guard Bureau Records Management Program"
- rr. DoD Senior Intelligence Oversight Official SIPRNET Websites, <SIPRNET: [intellipedia.intelink.sgov.gov/wiki/Intelligence_Oversight_Inspections_and_Best_practice](https://intellipedia.intelink.sgov.gov/wiki/Intelligence_Oversight_Inspections_and_Best_practices)s>, accessed 21 July 2022
- ss. Department of Justice, "National Criminal Intelligence Sharing Plan," October 2003
- tt. DoDI 5505.77, 19 December 2012, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities" Incorporating Change 1, Effective 29 November 2016

GLOSSARY

PART I. ACRONYMS

A2	Director of Intelligence (Air Force)
ARNG	Army National Guard
ATSD(PCLT)	Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency
CD	Counterdrug
CG	The Commanding General of the District of Columbia
CI	Counterintelligence
CNGB	Chief of the National Guard Bureau
CNGBI	Chief of the National Guard Bureau Instruction
CNGBM	Chief of the National Guard Bureau Manual
CRE	Chemical, biological, radiological, and nuclear response enterprise
DoD	Department of Defense
FI	Foreign intelligence
FISA	Foreign Intelligence Surveillance Act
FP	Force protection
G2	Director of Intelligence (Army)
GC	General Counsel
GEOINT	Geospatial intelligence
HUMINT	Human intelligence
IAA	Incident awareness and assessment
IAW	In accordance with
IG	Inspector General
IMINT	Imagery intelligence
IN	Unit intelligence officer
IO	Intelligence oversight
IP	Internet Protocol
ISR	Intelligence, surveillance, and reconnaissance
J2	Joint Director of Intelligence
JA	Judge Advocate
LEA	Law Enforcement Agency
MASINT	Measurements and signatures intelligence
MEDINT	Medical intelligence
MFR	Memorandum for record
MI	Military Intelligence
NG	National Guard
NG JFHQs-State	National Guard Joint Force Headquarters--State
NGB	National Guard Bureau
NGB-GC	Office of the General Counsel
NGB-J2	NGB Joint Intelligence Directorate
NGB-J2-IO	NGB Joint Intelligence Directorate Intelligence Oversight
NGB-J34	NGB Antiterrorism & Critical Infrastructure Protection Branch
NSA	National Security Agency
PUM	Proper use memorandum

QIA	Questionable intelligence activity
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
T32	Title 32
TAG	The Adjutant General
TSCM	Technical surveillance countermeasures
URL	Uniform Resource Locator
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USPI	U.S. 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 ee; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference hh.

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 dd; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference hh.

Certifying Official -- A National Guard field-grade officer or civilian equivalent in authority over the requesting individual who will verify and remain 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 instruction and other applicable policy.

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 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 also serves as the principal advisor 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 or not it is retained by the Component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. 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 Intelligence -- In accordance with reference ss information compiled, analyzed, or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Criminal Investigation -- In accordance with reference tt, 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 Components -- The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense Agencies, the Department of Defense field activities, and all other organizational entities in the Department of Defense.

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, and 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 and/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 (to include 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 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 -- Activity normally considered to be linked directly or indirectly to the intelligence field and activities outside the consolidated Defense intelligence program that respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national Intelligence Community tasking of systems that have a primary mission to support operating forces; train personnel for intelligence duties; provide an intelligence reserve; or be devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.

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 Bureau -- A joint activity of the Army National Guard and Air National Guard pursuant to reference ii. 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-Reimbursable Support -- The cost of providing services that are within the mission of the host activity and are provided to all customers and tenants, regardless of use, and for which individual use cannot be accurately measured.

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 U.S. 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 Locator 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).

Unintelligible Information -- Information that is not in an intelligible form, to include information that the National Guard intelligence component cannot decrypt or understand in the original format. Unintelligible information includes information that a Component cannot decrypt or understand in the original format.

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.