CHIEF NATIONAL GUARD BUREAU MANUAL

NGB-J2 CNGBM 2000.01A
DISTRIBUTION: A 11 April 2019

NATIONAL GUARD INTELLIGENCE ACTIVITIES

References: See Enclosure L.

1. Purpose. This manual provides procedural guidance for National Guard intelligence and intelligence-related activities in accordance with (IAW) the references.

2. Cancellation. This manual supersedes its previous edition, Chief of the National Guard Bureau Manual (CNGBM) 2000.01, 26 November 2012, "National Guard Intelligence Activities."

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

4. Procedures. References a through j give clear guidance for ensuring the legality and propriety of all intelligence, counterintelligence (CI), and intelligence-related activity. This manual applies references c through f to the NG intelligence component and gives specific guidance for conducting intelligence and intelligence-related activity and training through 13 procedures.

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

b. Procedures 5 through 10 define procedures regarding the use of special collection techniques to obtain information for foreign intelligence (FI) and CI purposes. Authority to employ these techniques is limited to that necessary to perform functions assigned to the 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. Employee Conduct (formerly known as Procedure 14). Employees of the NG intelligence component will conduct intelligence and intelligence-related activities only IAW references a through j, 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. Employees of the NG intelligence component will carry out reporting responsibilities as delineated in Enclosure C.

e. Identifying, Reporting and Investigating Questionable Intelligence Activity (QIA), Significant or Highly Sensitive Matters (S/HSMs), and Federal Crimes (formerly known as Procedure 15). The NG Intelligence Component is required to report misconduct incident to intelligence and intelligence-related activities that violates any executive order, 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 or authorized mission, authority, and purpose before conducting the activity.

5. Summary of Changes. This document has been substantially revised and must be completely reviewed. 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. Obtain copies through <https://www.ngbpdc.ngb.army.mil>.

7. Effective Date. This manual is effective upon publication and must be reissued, cancelled, or certified every five years.

PATRICK J. COBB
Brigadier General, USAF
Director, Joint Intelligence

Enclosures:

A -- Procedures
B -- Identifying, Investigating, and Reporting Questionable Intelligence Activity, Significant/Highly Sensitive Matters (S/HSM), 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 Social Media
I -- The IO Continuity Binder
J -- Compliance Inspection Guidance and Self-Inspection Checklists
K -- The 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 only pursuant to and IAW references a through j and this manual; personnel will not exceed the authorities granted by these references or by applicable laws, executive orders (EOs), regulations, instructions, or policies. All activities in all circumstances will be carried out IAW the U.S. Constitution and laws.

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 the Constitution 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. This includes dissemination of information to the White House. Furthermore, they will not participate in or request that 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 receipt of intelligence oversight training and agreement to comply with all law, policies, and procedures applicable to the protection of USPI. A sample acceptable use agreement is 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 in Procedures 2 through 4 of this manual. Any questionable intelligence activity (QIA) 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 pursuant to this issuance.

SAMPLE ACCEPTABLE USE AGREEMENT

I acknowledge that my access to and use of *insert name of shared repository* 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) Instruction 2000.01C and CNGB Manual 2000.01A, "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 Instruction 2000.01C and CNGB Manual 2000.01A. Furthermore, I agree to notify *insert repository host's name* of any restrictions to access and use applicable to any USPI that I provide.

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 protection of USPI (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 participating in a shared repository allow access to or use of USPI from the shared repository, they have made a dissemination. Therefore, allowing access to or use of USPI in this manner will be conducted IAW Procedure 4 below.

2. Procedure 2: USPI Collection.

a. Intentional Collection of USPI. 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 of information, below and in Table 1, and is 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 (COMSEC) investigations
Overhead and airborne reconnaissance* *A second category is required for collection under this category
Administrative purposes

Table 1. Categories of Information

(1) Publicly available USPI, which includes information concerning U.S. persons appearing in print or electronic form on the radio, on television, in newspapers, in journals, on the Internet, in commercial databases, and in videos, graphics, and drawings. An example is an NG JFHQs-State Joint Director of Intelligence (J2) collecting information detailing names, addresses, emergency exits, and the number of beds in local hospitals from public records for joint intelligence preparation of the operational environment during hurricane response.

(2) Information obtained with consent. Information may be collected about U.S. persons who consent to such collection. 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 search and rescue (SAR) exercise is an example. Consent is implied during a real-world SAR mission.

(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) Information 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 in, 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 in, 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) Information needed to protect the safety of any person or organization, including those who are victims, targets, or hostages of international terrorist organizations or individuals, and at least one of the following criteria is met:

(a) The threat has a foreign connection.

(b) NGB-J2 or NG JFHQs-State J2 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,

when the collection 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 NG or an NG contractor.

(7) Current, former, or potential sources of assistance to intelligence activities: information concerning those who are or have been sources of information or assistance, 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 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.

(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 or NG employees, installations, operations, or visitors. 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 have or be supporting an authorized physical security mission and must be able to articulate a reasonable belief in both the foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.

(11) Communications security (COMSEC) investigation: information arising from a lawful COMSEC inquiry or investigation.

(12) Overhead and airborne reconnaissance: information obtained from overhead or airborne reconnaissance, including information from unmanned aircraft systems (UAS) and remotely piloted aircraft (RPA) and imagery from overhead (satellite) or 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 or, if the collection is directed at a specific U.S. person, the collection falls in one of the other 12 categories.

(b) Collection of any domestic imagery must also comply with other applicable laws, policies, and procedures, including DoD and National Geospatial-Intelligence Agency (NGA) policy.

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

(13) Administrative purposes: information required for administrative purposes (for example, addresses and phone numbers for recall rosters).

b. 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.

c. 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.

d. 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.

(2) NGB-J2, through the NG JFHQs-State J2, will review and approve all proposed NG intelligence component special circumstances collection. If advance authorization is not possible, then, as soon as possible after collection, NGB-J2, through the NG JFHQs-State J2, 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. NGB-J2 or the NG

JFHQs-State J2 will consult the appropriate Judge Advocate (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 in accordance with 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.

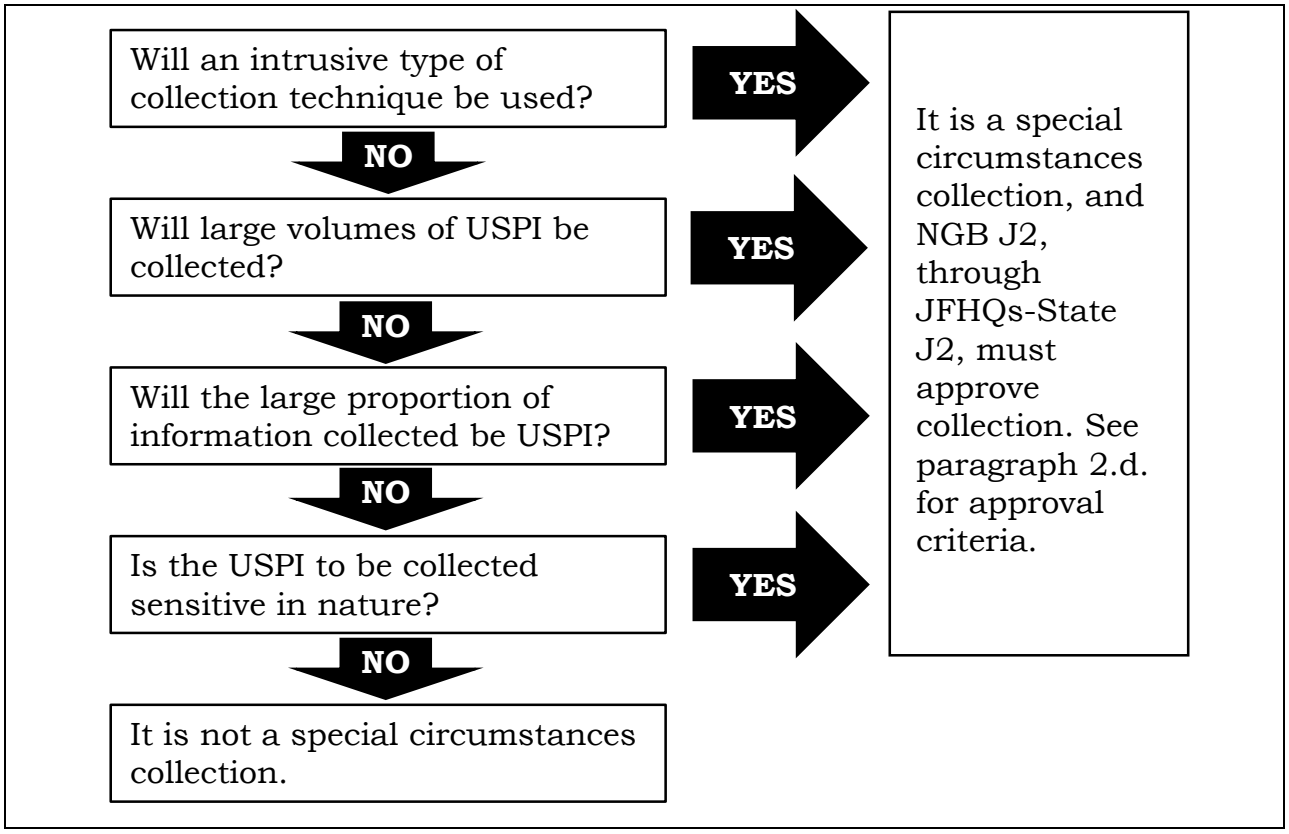

Figure 2. Does the Collection Constitute Special Circumstances Collection?

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

(1) Means of Collection. NG intelligence component elements may collect USPI by any lawful means, provided that all such collection activities are carried out in accordance with references a through c and this manual.

(2) Restriction on Purpose. 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 the Constitution or laws of the United States.

(3) Least Intrusive Means. 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.

(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 NGB-J2 and JA to the DoD General Counsel (GC) for the use of intelligence collection techniques that require a judicial warrant or approval from the Attorney General.

f. Limitations on FI collection Within the United States. Within the United States, FI concerning U.S. persons may be collected 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 or NG 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 or NG intelligence component.

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

(d) The use of any other sources and methods has been approved by the appropriate T-10 authority. A copy of any approval granted IAW this procedure will be provided through NGB-J2 to the Under Secretary of Defense, Intelligence (USD(I)).

g. Date and Time Stamp. All USPI collected by the NG intelligence component 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.

h. 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 or 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 2.

Name	E-mail Address
Address	Phone Number
IP Address	Social Security Number
Physical Description	Driver's License Number
Date of Birth	Place of Birth

Table 2. Examples of USPI

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

a. Intentionally collected USPI. NG 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 NG intelligence component may retain the USPI for evaluation for up to five years. The NGB J2 or NG JFHQs-State J2 may approve an extended period in accordance with Paragraph 3.e below.

b. Incidentally Collected USPI. In the course of routine duties, an NG intelligence component element many 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 NG intelligence component element may retain all of the incidentally collected information for evaluation for up to five years. NGB-J2, through the NG JFHQs-State J2, 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 NG 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 NG intelligence component receives information that is voluntarily provided about a person reasonably believed to be a U.S. person, the NG intelligence component element will evaluate the information promptly. If necessary, the NG intelligence component element may retain the information for evaluation for up to 5 years. NGB-J2, through the NG JFHQs-State J2, may approve an extended period in accordance with paragraph 3.e below. If an NG 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 NG 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 NG intelligence component element conducts a special circumstances collection in accordance with Procedure 2.e, the NG 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) 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 Retainability Determination	Extension
Intentionally collected USPI	Inside or outside the U.S.	Promptly, or up to 5 years if necessary	5 years Approved by NGB or State J2 May be given at time of collection or later
Incidentally collected USPI	Inside the U.S.	5 years	5 years Approved by NGB or State J2 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 NGB or State J2 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) 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. NGB-J2, referred to as the "official" in paragraphs 3.e(1)(a), (b) and (c) below, through the NG JFHQs-State 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 the retention is necessary to carry out an authorized mission of the NG intelligence component element, and the retaining NG 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.

(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 NG intelligence component element is authorized to collect in accordance with 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 in accordance with Paragraph 3.d.

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

h. Deletion of USPI. NG intelligence component elements will delete all USPI, including any information that may contain USPI, that does not meet the permanent retention criteria from the NG 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 NG 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 NG intelligence component element must evaluate the information for permanent retention within a reasonable time.

j. Permanent Retention.

(1) Retention standard: An NG intelligence component element 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 by the NG intelligence component element 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 collected by an element of the NG intelligence component incidentally to authorized collection or disseminated to an element of the NG intelligence component 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 NG 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 (SIOO), a Component Inspector General (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)	• Intentional • Incidental • Voluntarily provided • Special circumstance • Disseminated by another DoD Intelligence Component or Intelligence Community element
4. If disseminated by another DoD Intelligence Component or Intelligence Community element, which one?	
5. Location of U.S. person(s) when collected	
6. Authorized mission supported	
7. Why it is reasonably believed to be necessary to permanently retain the USPI	
8. Approved category(ies) of information under which the USPI falls (circle all that apply)	• Publicly available information • Information obtained with consent • Information reasonably believed to constitute Foreign intelligence • Counterintelligence • Threats to safety • Protection of intelligence sources and methods • Current, former or potential sources of assistance to intelligence activities • Persons in contact with sources of potential sources • Physical security • Personnel security • Communications security (COMSEC) investigation • Overhead and airborne reconnaissance (not for targeting specific US persons) • Administrative purposes
9. Means of collection	

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

[J2/G2/A2SIO/Commander signature block]

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	
7. Describe why it is reasonably believed to be necessary to permanently retain the USPI	
8. Approved category(ies) of information under which the USPI falls (circle all that apply)	• Publicly available information • Information obtained with consent • Information reasonably believed to constitute Foreign intelligence • Counterintelligence • Threats to safety • Protection of intelligence sources and methods • Current, former or potential sources of assistance to intelligence activities • Persons in contact with sources of potential sources • Physical security • Personnel security • Communications security (COMSEC) investigation • Overhead and airborne reconnaissance (not for the purpose of targeting specific US Persons) • Administrative purposes
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. *[J2/G2/A2SIO/Commander signature block]*	

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

l. 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 the 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. NG 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 XXX."

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 a 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. IO 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 that 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 2000.01A, "National Guard Intelligence Activities"

1. I certify that, in accordance with Enclosure B, paragraph 3.l of the reference, the *UNIT* 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 Procedures 2 and 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 1.

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.	
Other Intelligence Community elements	Dissemination is for the purpose of allowing the recipient to determine whether the information is relevant to its responsi-bilities and can be retained.	
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.	
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.	NGB-J2 or the State J2 must approve any dissemi-nation 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.	NGB-J2 or State J2 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 delegatee 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.	NGB-J2 or the State J2 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 NGB-J2: (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 NG.

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, NGB-J2 or the State J2 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.	

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

c. Disseminations Requiring Approval. Any dissemination that does not conform to the conditions set forth in this procedure must be approved by NGB-J2 or the Deputy J2 on the advice of the Office of the NGB Chief Counsel (NGB-JA) 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.

d. 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.

e. Improper Dissemination of USPI. Any improper dissemination or suspected improper dissemination of USPI will be reported immediately upon discovery IAW Enclosure B and reference 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 real-world SIGINT collection activities. Under no circumstances may units perform real-world 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 the U.S. Constitution. Units involved in SIGINT will be aware of and comply with applicable NSA/Central Security Service United States Signals Intelligence Directives (USSIDs), which include references m through r.

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 T-10 status. Commands that have SIGINT cryptologic elements will ensure that those elements conduct activities IAW applicable USSIDs, such as references n through r. 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. 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 either real-world 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 e-mail to:

- the G-TCAE at ng.ncr.ngb.mbx.g2-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) in reference s, the NGB-J2 TSCM team may conduct their activity only IAW references e and t. 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:

(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 counter-measures are to be undertaken.

(d) If the use of TSCM constitutes electronic surveillance as that term is defined in reference u, 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 that term is defined in reference u to protect information from unauthorized surveillance or to enforce references v and w. 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 that term is defined in reference u, 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.e above or for collection avoidance purposes. The technical parameters will be maintained in accordance with 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 T-32 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. Army National Guard (ARNG) CI elements in a T-32 status are not authorized to conduct physical searches of any person or property in the United States.

b. Physical searches outside the United States. ARNG CI activity performed outside the United States must be conducted in T-10 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 T-32 status are not authorized to search mail or to request and use mail covers. These activities must be conducted in T-10 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 T-10 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.

a. 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. When non-disclosure of intelligence component sponsorship is necessary in contracts for enrollment of students in academic institutions, the provisions of Procedure 10 apply.

b. 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.

c. 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 ANG) 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, tribal, or local civilian law enforcement agency (LEA).

a. Requests for NG military support to civilian law enforcement (LE) 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 an LEA under the authority of reference hh)	SecDef or appropriate 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 an LEA (as an incidental or secondary purpose)	Operating under T-32 training authorities for the primary purpose of intelligence training	SecDef or appropriate approval required

Table 5. Approval Authority for LEA Support

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

(2) Intelligence-Related Activities. When the request for support to a civilian LEA involves leveraging intelligence training to meet an incidental benefit of law enforcement support, it is 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 J34, force protection (FP), or LE 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.

d. Requests for support requiring SecDef approval under this procedure will be staffed from the NG JFHQs-State J2 to NGB-J2. The following documents are required: a request for assistance from the LEA, a request for SecDef approval from TAG, 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 LEA. An electronic template is available for download on the NGB-J2 IO website, reference x.

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 k. 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, NGB-J2, JA, or IG channels by procedures identified in reference k.

a. QIA. IAW reference c, 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 is QIA.

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 a QIA in this context 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 LE channels. NGB-J2, NGB-JA, or NGB-IG; the NG JFHQs-

State J2, JA, or IG; or ARNG unit intelligence officer (S2) or ANG unit intelligence officer (IN or 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 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:

(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 LE investigation and proper search or electronic surveillance authority.

g. Creating a fake social media account to monitor the activity of a U.S. person during NG civil support.

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

(1) Falsifying investigative reports or personnel security investigation interviews (also known as “curbstoning”).

(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 references b, c, y, and z. 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 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 T-32 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 DoD SIOO.

d. Examples of reportable Federal crimes: espionage, sabotage, un-authorized 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) Other than 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)/imagery intelligence (IMINT), SIGINT, human intelligence (HUMINT), open-source intelligence (OSINT), measurements and signatures intelligence (MASINT), and medical intelligence (MEDINT).

2. GEOINT/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. The NSA is the only organization that can authorize real-world SIGINT collection. Under no circumstances may units perform real-world 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 aa. Units involved in SIGINT will be aware of and comply with applicable NSA/Central Security Service directives and policies, which include references m through r, because they dictate performance boundaries within SIGINT training and operations. ARNG exercise SIGINT must follow reference r. Exercise SIGINT (LLVI, Prophet, etc.) 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 witting and unwitting. HUMINT collection activities include conducting source operations; liaising with host nation officials and allied counterparts; eliciting 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. T-32 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.

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.

7. MEDINT. MEDINT is the collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information of interest to 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. T-32 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 has no independent authority to engage in real-world CI activity.

ENCLOSURE D

INTELLIGENCE OVERSIGHT TRAINING REQUIREMENTS

1. Training Requirements.

a. The following personnel must receive IO training:

(1) All NGB, T-32 NG JFHQs-State, and T-32 NG intelligence staff organizations and units, as well as T-32 non-intelligence organizations that perform intelligence or intelligence-related activities, as defined in the glossary, also known as the NG intelligence component.

(2) All T-32 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 T-32 NG units and staffs that conduct information operations, which includes cyberspace intelligence activities.

(5) All T-32 NG non-intelligence units and staffs, such as Eagle Vision, running systems that acquire and disseminate commercial satellite products to intelligence units and staffs.

(6) All TAGs 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 (TDY) Training. IO monitors will ensure all personnel deploying to another duty location retain currency for the duration of the deployment or TDY. If currency is scheduled to lapse during the deployment or TDY, 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 (T-10, T-32 or State active duty [SAD]) 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.

(8) Staff, 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) Special focus areas, such as the use of the intelligence component for NG civil support or domestic operations missions, intelligence support to FP, use of the Internet, and use of social media, applicable to the staff, unit, or organization.

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

b. Resources. To develop tailored training, units may download data from the folders on the NGB-J2 IO Guard Knowledge Online website (reference x). The DoD SIOO provides IO training resources to assist in developing unit-specific IO training at reference bb.

4. Additional Training Requirements for SIGINT Units. Commands with SIGINT elements will ensure that those elements obtain appropriate training from qualified personnel on applicable SIGINT directives. Reference e also requires training on the requirements and restrictions of the Foreign Intelligence Surveillance Act (FISA) (reference u) and EO 12333 (reference 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 T-10 status.

ENCLOSURE E

DOMESTIC OPERATIONS

1. Homeland Defense (HD). Certain NG units support HD missions, including air defense of the homeland and anti-missile defense of the homeland. Mission and authority for NG intelligence activities include conducting these HD 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. In this regard, the determination of compliance with IO guidance can be complex; when in doubt, seek unit, State, or NGB-JA guidance. Several topics to consider: Is there a foreign connection? Is it part of the element's mission-essential task list? Is it within the purpose of the funding being used? Are the activities overt and transparent? And, finally, has any USPI been properly safeguarded and have rights to privacy been protected?

3. National Guard Civil Support. NG intelligence component personnel may leverage T-32 training to provide incidental support to their State mission with non-intelligence equipment to fulfill TAG 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. Federal intelligence or Federal ISR equipment may be used only when approved by the SecDef, the SecDef's designee, or an appropriate approval authority or as directed by the President.

a. SAR. Upon a local, tribal, or State request, or a request by the Air Force Rescue Coordination Center, the Title 32 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 UAS or RPA].) USPI may be collected during SAR missions; if a person is at risk of death or injury, consent to gather intelligence is implied. However, once the SAR mission is over, all USPI will be purged. Standing SAR PUMs and DILRs are filed each fiscal year for use on non-intelligence equipment for SAR. Each approved use of Federal ISR equipment for SAR requires a separate PUM.

b. IAA. NG intelligence component personnel and non-intelligence equipment may be used for IAA to fulfill TAG 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, or tribal agency for the event; an Emergency Management Assistance Compact (EMAC) request; or a Mission Assignment from the Federal Emergency Management Agency (FEMA).

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

(2) Processing, assessment, and dissemination. During domestic operations, the NG T-32 intelligence component may use unclassified equipment to process, assess, and disseminate final products based on that analysis of:

(a) Imagery, geospatial data, and information collected from cameras, video, electro-optical sensors, IR, and forward-looking infrared radar (FLIR) 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 T-32 intelligence component may use Federal intelligence equipment to process, assess, and disseminate final products within the parameters set by the SecDef.

(4) National Guardsmen many use only approved official 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. 32 U.S. Code § 112 -- 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 cc, drug interdiction and CD activities with respect to the T-32 NG mean "the use of NG personnel in drug interdiction and CD law enforcement activities, including drug demand reduction activities, authorized by the law of the State and requested by the Governor of the State."

(2) Intelligence and intelligence-related activity is not authorized under reference cc 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 the Guardsmen are operating are not exceeded. See references cc and dd for additional information.

(3) NG personnel providing criminal analysis support, a non-intelligence activity, to civilian LEAs under the authorities of reference cc and the approved State CD plan, will comply with references ee and ff. 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 intelligence files or databases.

(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 NG MQ-9 Reaper RPA to support the State plan requires separate geographic combatant commander approval under reference gg.

b. 10 U.S. Code § 284 -- Support for CD Activities and Activities to Counter Transnational Organized Crime – DoD Support. When approved by the SecDef or designee, the T-32 NG intelligence component may provide intelligence support to Federal agencies, such as the Drug Enforcement Administration, under the authorities of reference hh. 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. All NG CD programs will maintain an IO program. The IO Monitors will ensure that States are not conducting unauthorized intelligence or intelligence-related activity.

5. The NG CBRNE Response Enterprise (CRE). NG Weapons of Mass Destruction–Civil Support Teams, CBRNE 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 outlined in references ee and ff concerning the handling of information related to persons not affiliated with DoD. However, intelligence personnel assigned to intelligence billets to provide intelligence support to these units have the mission and authority to support emergency response, to collect information to prepare for possible response, and to perform effective research, analysis, and threat assessment. Intelligence personnel will comply with the provisions outlined in reference a and this manual. While conducting operations, CRE units could incidentally or otherwise collect USPI. Upon completion of operations, all information or files must be redacted of all USPI 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 outlined in this manual and reference a.

7. Cyber Intelligence. T-32 NG personnel assigned to cyber intelligence and cyber ISR units and billets are subject to this manual and references a through f. This includes T-32 National Guardsmen filling intelligence billets on 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 joint intelligence preparation of the operational environment and 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 references a and 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. Legal Requirements. IAW reference ii, the following generally constitute legally valid requirements for domestic imagery:

(1) Natural or man-made disasters. This includes requirements to conduct IAA in support of government planning for emergency response to, or recovery from, events such as tornadoes, hurricanes, floods, mudslides, fires, oil spills, and chemical spills.

(2) CI, counterterrorism, and security-related vulnerability assessments. This category of information supports critical infrastructure analysis on Federal property, or State or private property where consent has been obtained as appropriate.

(3) Requirements in support of environmental studies of wildlife, geologic features, forestation or similar scientific, agricultural, or environmental studies not related to regulatory or LE actions.

(4) Exercise, training, testing, or navigational purposes. Requirements for imagery coverage of property solely in the conduct of NG exercises, training, and testing or for navigational purposes.

(5) Systems testing, engineering, and research and development. This supports requirements for imagery coverage in support of system or satellite calibration, satellite pre-launch and post-launch contingency operations, algorithm or analytic development, and training or weapons systems development or training.

2. Domestic Imagery from National Satellites. The NGA is responsible for the policy and legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites. IAW references ii through kk, the NG intelligence component must submit requirements for new collection to the NGA through NGB-J2 (for T-32) or the gaining combatant command (COCOM) or major command (for T-10). 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. An approved PUM or DILR must be on file with NGB-J2 (for T-32) or the gaining COCOM or major command (for T-10) 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 T-32 NG for intelligence, intelligence-related, or IAA purposes.

d. Refer to Table 6 and Figure 8 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)	Intelligence activity (for example, ISR for FI/CI purposes)	PUM
Non–Intelligence Component Capability (for example, A-10, F-15, F-16, UH-60, or UH-72)	Intelligence activity (for example, non-traditional intelligence, surveillance and reconnaissance [NTISR] for FI purposes)	PUM
Intelligence Component Capability (for example, JSTARS, MC-12, MQ-9, RQ-7, or RQ-11)	Intelligence-related activity (for example, ISR training)	PUM
Non–Intelligence Component Capability (for example, A-10, F-15, F-16, UH-60, or UH-72)	Intelligence-related activity (for example, training for intelligence, surveillance or reconnaissance)	PUM
Intelligence Component Capability (for example, JSTARS, MC-12, MQ-9, RQ-7, or RQ-11)	Non-intelligence activity	PUM
Non–Intelligence Component Capability (for example, A-10, F-15, F-16, UH-60, or UH-72)	Non-intelligence activity	DILR

Table 6. Domestic Imagery Collection Documentation

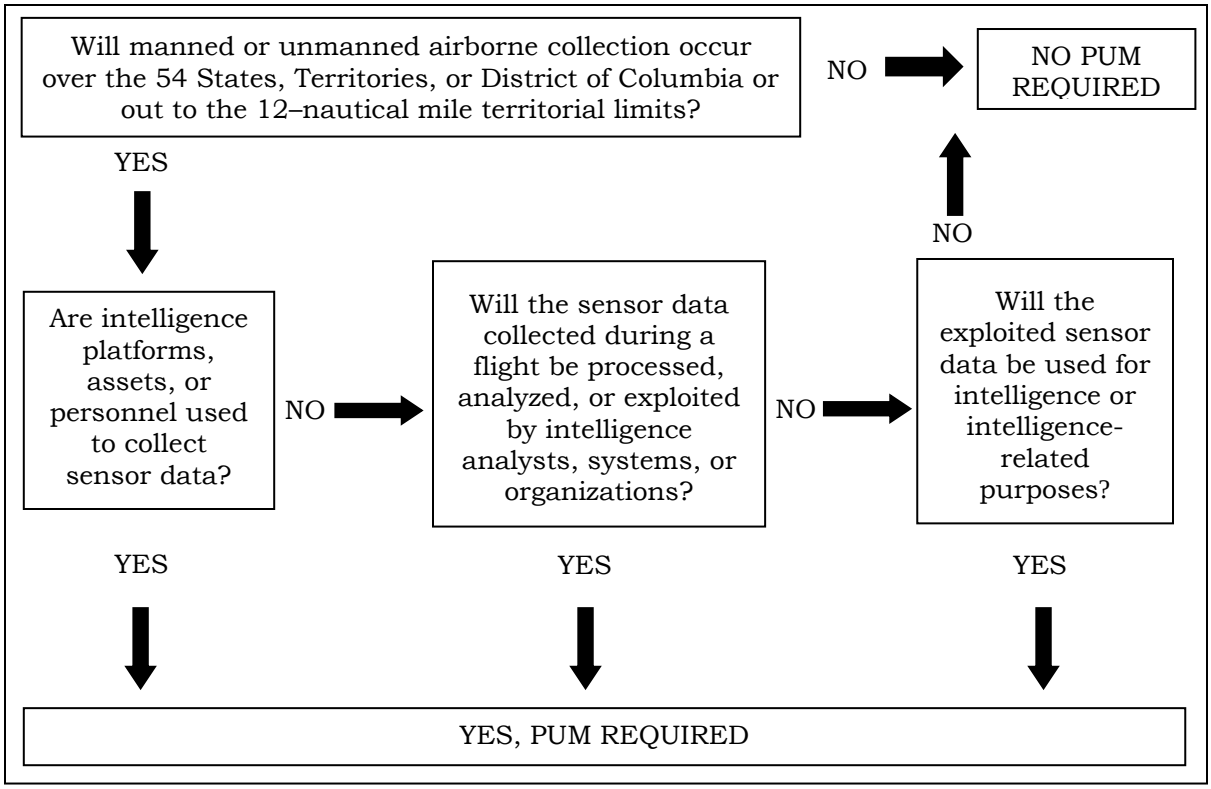

Figure 8. Is a PUM Required?

4. CD PUMs. PUMs are not required for domestic imagery collection missions flown in support of a LEA under the approved State CD plan so long as the following three criteria are met (the use of UH-72 and RC-26 sensors for other purposes, such as IAA, likely requires a PUM):

a. The equipment being used for CD missions is CD-funded equipment (in other words, the UH-72 or RC-26) by aircrews on CD-funded orders and is not ISR equipment or UAS or RPA (such as the MC-12, JSTARS, MQ-9, RQ-7, or RQ-11).

b. The analysis of the images collected is done by members assigned or detailed (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. All PUMs must be filed IAW this paragraph 6 below.

5. Domestic Imagery from Commercial Satellites.

a. NG intelligence component elements may obtain archived NGA 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, and domestic disaster relief operations, in either T-10 or T-32 status. NG intelligence component elements may also use domestic open-source, publicly available, and other commercial imagery (for example, U.S. Geological Survey [USGS] imagery, Eagle Vision, Google Earth imagery, and Falcon View imagery). However, the onus of compliance with IO and other policies is on the user. Therefore, 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 can be found in Figure 9. The NG intelligence component 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 (e.g., NG-J2 2014)* Commercial Domestic Imagery and Other Geospatial Information Use Authorization

1. (U//FOUO) In accordance with Chief of the National Guard Bureau Manual 2000.01A, "National Guard Intelligence Activities," Enclosure G, paragraph 4, 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 (e.g., 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 (e.g., military training, exercises, defense support of civil authorities, incident awareness and assessment, joint intelligence preparation of the operational environment, vulnerability assessments, and other real-world 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-J2 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; e-mail; or hand delivery.)*

4. (U//FOUO) "I certify that the intended collection and use of the requested information, materials, and imagery are in support of Congressionally approved programs and are not in violation of applicable

Figure 9. Internal MFR Certifying Proper Use of Commercial Domestic Imagery

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 ii 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, RPA, and UAS 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. Civil LEAs, such as U.S. Customs and Border Protection, the FBI, 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, NG ISR, fighter and bomber, RPA, and UAS assets equipped with electro-optical, IR, 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, FAA approval for UAS and RPA 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.

(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. NG UAS and RPA use must comply with the policy in references gg and mm.

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

a. PUM and DILR.

(1) PUMs can be classified or unclassified, depending on content. The PUM 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 civilian equivalent, who will verify and remain accountable for the accuracy of the domestic imagery request. The PUM provides an auditable trail of authority and responsibility up to the appropriate levels, while ensuring that the rights of U.S. citizens and organizations are being protected IAW the law. Failure to file a PUM before conducting a domestic imagery collection mission is QIA, reportable IAW procedures established in reference k.

(2) 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 before executing a domestic imagery collection mission. In a T-32 status, the JFHQs-State J2 will route PUMs to NGB-J2 as outlined in paragraph 6.a(6) below. NGB-J2 will forward the PUM to NGB-JA for review. Once the document is found to be legally sufficient, NGB-J2 will approve the PUM and notify the requesting State. In a T-10 status, the gaining COCOM or major command J2, A2, or Army Director of Intelligence (G2) is responsible for the PUM.

(3) One-time or one-year requests. A PUM may be written as a one-time or one-year request. One-year requests cover routine training in routine training areas. Any training or exercises beyond the scope of this routine training or real-world missions require separate PUMs (for example, IAA missions in support of the Kentucky Derby, IAA missions in support of hurricane response efforts, and training missions in support of a Vigilant Guard exercise).

(4) PUMs will include the following:

(a) Subject Line. Identify the document as an NG T-32 PUM for a domestic imagery request. The majority of PUMs will be T-32 training PUMs; however, if it is an approved T-32 operational mission, the PUM will state that. Include the dates on which collection will occur.

(b) Paragraph 1: References. Include all applicable intelligence oversight and domestic imagery policy documents.

(c) Paragraph 2. State in nontechnical terms 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. Include either:

1. The following statement that no U.S. persons will be targeted: "No U.S. persons will be targeted during these missions. Any personally identifying information unintentionally and incidentally collected about specific U.S. persons will be purged and destroyed unless it may be lawfully retained and disseminated to other governmental agencies that have a need for it in accordance with applicable laws, regulations, and policies."

2. Which U.S. person(s) will be targeted; attach letter(s) of consent.

[Print on company letterhead]

[Insert date]

The *[Insert the corporation's name]* hereby gives consent for the U.S. Government to take overhead photographs and collect remotely sensed data and to use such information for U.S. Government purposes. As President of *[Insert the corporation's name]*, I am authorized to provide this consent. I understand that the photography and data collection will take place between *[Insert the dates as Day Month Year (DY MON YEAR)* and *(DY MON YEAR)]*.

[SIGNATURE]
[Title]

Figure 10. Private Corporation Letter of Consent

a. Private Corporation letter of consent. Not all situations require letters of consent. Examples of situations that may require a letter of consent: imagery of a privately owned nuclear power plant, imagery of a privately owned levee, or imagery of privately owned fairgrounds. If in doubt, please contact NGB-J2 to discuss the named areas of interest for collection. If a letter of consent is required, it must be on corporate letterhead. The letter of

consent may also identify the intended use of the photography or remotely sensed data; however, identification of a specific use may also limit other uses unless an additional letter of consent is obtained. The longest permissible duration of a letter of consent is one year. See Figure 10 for a template.

b. Private individual letter of consent. Examples of situations that may require a letter of consent: imagery of a citizen's farm or imagery of a local business. If in doubt, please contact NGB-J2 to discuss the targets of intent. The letter of consent may also identify the intended use of the photography or remotely sensed data; however, identification of a specific use may also limit other uses unless an additional letter of consent is obtained. The longest permissible duration of a letter of consent is one year. See Figure 11 for a template.

[Insert date]

I, *[Insert the individual's name]*, hereby give my consent for the U.S. Government to take overhead photographs and collect remotely sensed data of my *[Insert the target (for example, levee, grain silo)]* and surrounding area, located at *[Insert the address]*, and to use such information for U.S. Government purposes. I understand that the photography and data collection will take place between *[Insert the date as Day Month Year* (DY MON YEAR) and DY MON YEAR*]*.

[SIGNATURE]

Figure 11. Private Individual Letter of Consent

(e) Paragraph 4. Specify the organizations and equipment that will process and exploit, analyze, and disseminate the imagery and sensor data, and for what purpose. Include the organizations that are to receive the imagery (or derived products, briefings, or publications) and the desired format; retention information (where the imagery will be stored); disposal procedures; and certification that IO training has been given.

1. Identify each user organization, even if a large number of organizations are involved. Use of 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 (digital, tape, paper print, duplicate positive, negative, etc.).

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

(f) Paragraph 5. Judge Advocate review. Include the following:

1. Proper Use Statement: "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. 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. This PUM has been reviewed for legal sufficiency by *[insert rank, name, title, e-mail address and phone of Staff Judge Advocate reviewing the PUM]* on *[insert date reviewed]*.

(g) Paragraph 6. State J2 certification (must be a field-grade officer in the rank of major or above, or civilian equivalent): "Certification: 'I am authorized as a trusted agent and certifying official on behalf of the requesting unit, and I understand I am responsible for the accuracy of the information herein and for the proper safeguarding of products received in response.' Insert State J2 POC and contact information—must be field-grade officer or civilian equivalent." If the NG JFHQs-State J2 does not meet the rank requirements, a field-grade officer in the rank of major or above in the J2's chain of command is authorized to sign.

(h) Paragraph 7. Name, office, telephone number, and e-mail address or fax number for the PUM 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-State J2 does not meet the rank requirements, a field-grade officer in the J2's chain of command is authorized to sign.

(5) Current PUM templates are available for download on the NGB-J2 IO website, reference x.

(6) Staffing procedures for T-32 airborne platform PUMs rules:

(a) Approval resides with NGB-J2.

(b) Requests will be submitted 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 prior to the first day of collection.

(c) Immediate approval authority. In a direct and immediate emergency in which time precludes obtaining an approved PUM before collection, TAG may authorize airborne domestic imagery collection, including the lawful acquisition of USPI when that support is consistent with the Constitution 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 Coordination Center. A PUM will be filed with NGB-J2 as soon as possible thereafter.

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

(e) For situational awareness, the NGB-J2 IO Section will provide to U.S. Northern Command a copy of PUMs covering natural or man-made disasters, National Special Security Events, or Special Event Assessment Rating events for which U.S. Northern Command may have interest or equities.

b. Commercial Domestic Imagery Proper Use Internal Memorandum for Record (MFR). The Proper Use 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 Proper Use Internal MFR should be retained on file one year after its expiration. It may be recertified if the imagery is still required. See Figure 9 or the NGB-J2 IO website, reference x, for a template.

8. Dissemination of Domestic Imagery.

a. Distribution of domestic imagery to parties other than those identified in the approved PUM is prohibited unless the recipient is reasonably perceived to have a specific, lawful governmental function requiring it (see Procedure 4). Adding users to the original PUM is accomplished by submitting an amendment to the PUM. See the NGB-J2 IO website, reference x, for a PUM amendment template. Domestic imagery used in briefings, reports, or publications may not be used for any purpose other than that for which it was originally requested.

b. Unless otherwise approved, domestic imagery must be withheld from all general access database systems. Controlled or limited access shared folders or drives, password-protected websites, password-protected portals, and e-mail 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, 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.

9. 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 will not be analyzed unless approval is granted IAW the PUM process (that is, through approval of an amendment to the original PUM).

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

c. A requesting organization must clearly communicate in its PUM who the exploitation 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 exploitation of imagery of a sensitive Federal named area of interest.

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

10. Public Affairs Use of Domestic Imagery.

a. Media and public interest in NG domestic operations, including IAA, can be intense and immediate. Participants in IAA will coordinate with the unit or organization public affairs officer on any requests for information. Personnel should 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 freely 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 onward 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. Specific imagery products may be released to the U.S. media during senior official press conferences to depict disaster area status and disaster response activities.

c. Civil authorities are authorized to disclose (that is, show) or release selected unclassified imagery products For Official Use Only (FOUO) to participating or affected private citizens when the disclosure or release 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 FP may involve identifying, collecting, reporting, analyzing, and disseminating intelligence regarding foreign threats to the NG, thereby enabling commanders to initiate FP measures. If during the course of routine intelligence 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, and local LE authorities. In the United States, the NG intelligence component will limit FP collection to FI and international terrorism threat data. The NGB and NG JFHQs-State Provost Marshal (PM) or J34 provide NG leadership with information and recommendations to support decision-making pertaining to FP, critical infrastructure, security, and LE activities. This activity requires review, analysis, and distribution of significant and relevant LE information. The NGB, NG JFHQs-State PM, and 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 references ee and ff.

b. However, when foreign groups or persons threaten DoD personnel, resources, or activities, the NG intelligence component may intentionally collect, retain, and disseminate this information.

c. NG intelligence personnel may receive information from LEAs, other organizations, or sources that contain U.S. persons' information. However, 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.

d. IO provisions do not prohibit States from calling meetings or even establishing "information fusion cells" or "threat working groups" where representatives from intelligence, CI, security, and LE meet to share and synthesize information to support the FP mission. Security, FP, or LE, not intelligence personnel, should lead the meeting.

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

United States. NG intelligence component elements that are assigned an FP mission may collect USPI only IAW the procedures in this manual and reference e. Coordinate with the appropriate LE unit or agency before collecting information on any U.S. individual or domestic group for FP purposes.

f. When an NG unit's specified mission is security operations in support of an LE mission, all information obtained on persons and organizations not affiliated with DoD that does not indicate a direct threat to DoD forces, facilities, or operations will be treated as the supported LEA's information. It will not be disseminated outside of the unit without the permission of the lead agency. All Non-DoD affiliated persons information must be purged, destroyed, or provided to the appropriate agencies, IAW applicable regulations and laws, once the NG mission has been concluded.

g. NG intelligence assets with the mission to support FP may assist in fusing LE, CI, and intelligence information in support of FP (for example, AT or LE activities), consistent with IO procedures. Criminal information containing USPI that does not indicate a direct threat to DoD forces, facilities, or operations will be passed to the appropriate Federal, State, local, or tribal LEAs and will not be retained by NG personnel. NG FP personnel are authorized to receive criminal information if there is no specific USPI or if the USPI is redacted, even if no direct threat to the NG exists but the LEA or Intelligence Community agency has included the information in threat summaries or intelligence products because that nonspecific information is necessary to an NG mission. For instance, a State fusion center report may include information on a new improvised explosive device technique used by a U.S. white supremacy group. The NG JFHQs-State J2 may then refer to the new method of making the explosive but redact the USPI.

h. With appropriate approval, aerial platforms and technology may be used to detect direct threats to DoD forces, facilities, and operations. Information on persons and organizations not affiliated with DoD and with no direct threat to DoD forces, facilities, or operations will not be retained but may be passed to LEAs. Cameras, video, and electro-optical, IR, and FLIR data may be placed on fixed objects as perimeter security around DoD forces and facilities to detect direct threats to DoD forces, facilities, and operations. Information on non-DoD persons and organizations that pose no direct threat to DoD forces, facilities, or operations may be passed to LEAs but not retained.

2. Dual-Hatting Intelligence, FP, or PM Personnel.

a. When personnel are not available, it is permissible to dual-hat intelligence and FP or PM personnel, but this is highly discouraged given the potential for IO violations and the risk of potential QIA. Consolidated

databases and files are not permitted. A clear separation between intelligence, FP, and PM channels must be maintained.

b. This paragraph does not apply to National Guardsmen who have different jobs as technicians and drill status, and use different systems, e-mail 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 a QIA or another 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 or 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, PM, the FBI, or the municipal police department) with authority to counter the threat.

c. Absent an imminent threat, reporting should be limited to J34, which will forward the information to other authorities as appropriate.

d. Threat information may be withheld from dissemination only upon the approval of the Department of the Army G2 or A2 for FI or Army Counterintelligence Coordinating Authority or the Commander, Air Force Office of Special Investigations, for CI, and only for national security reasons.

ENCLOSURE H

THE INTERNET AND SOCIAL MEDIA

1. General.

a. NG intelligence component elements must have official mission requirements before collecting, retaining, or disseminating even publicly available information about U.S. persons. Certain Internet-based activities are restricted by the rules requiring disclosure of an individual's intelligence organization affiliation. This applies to information found on the Non-secure Internet Protocol Router Network (NIPRNET), SIPRNET, Joint Worldwide Intelligence Communications System, and other classified media.

b. To properly apply IO provisions to the use of the Internet, intelligence and CI personnel must understand how to analyze as well as characterize Internet Protocol (IP) addresses, Uniform Resource Locators (URLs), and e-mail addresses.

2. Internet Protocol (IP) Addresses. As is the case with a telephone number, the numeric string comprising 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 very 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 quite 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 upon 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 obliged 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 any given IP address is associated with a U.S. person, then it may apply the presumption 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. If, however, the NG intelligence component subsequently obtains information to indicate 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. Even if an inquiry reveals that an IP address is assigned to a U.S. service provider, that is not necessarily sufficient information to require a presumption 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.

b. Some Internet service providers (ISPs) 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. E-mail Addresses. E-mail addresses, unlike both IP addresses and URLs, are nearly universally associated with individuals. It is often difficult, however, to identify the individual with whom any given e-mail address is associated. Some e-mail addresses are configured as a string of alphanumeric symbols that do not convey any meaningful information (for example, smitgj@ or smi2345@). Others plainly identify an individual (for example, George.Smith@). Regardless of how straightforward an e-mail address appears to be, more often than not, it 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 e-mail 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 e-mail address is associated with a U.S. person. The information to the right of the "@" represents the service provider. Some service providers predominately serve a non–U.S.-based clientele, and e-mail 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 e-mail 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 e-mail addresses may be collected, retained, or disseminated only IAW the requirements of references e and oo.

b. All other e-mail addresses may be treated similar to the approach described for the treatment of IP addresses. E-mail 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 e-mail addresses to assist the component in identifying them. Instead, the component must rely principally upon traditional methods to try to determine whether a given address is being used by a U.S. person.

c. For e-mail 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 e-mail 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.

4. Uniform Resource Locator (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 (the domain). If the domain is one 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 thus do not inform the determination 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 further 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 such collection is within the scope of an authorized intelligence or CI activity assigned to that component. NG intelligence component elements also may 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 (PII), 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; we assume the individual wants to be rescued. All PII must be destroyed immediately following the conclusion of domestic operations.

b. Under no circumstances may National Guardsmen use personal social media accounts for official purposes. Only general search engines or organizational accounts may be used. Organizational accounts must be established through the servicing public affairs office. Official on-line posts involve content released in an official capacity by an NG public affairs office.

ENCLOSURE I

IO CONTINUITY BINDER

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

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

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) -- maintain for three years. Use Service-specific systems of record for maintaining IO training records (that is, Document 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 k, this manual, and the State IO standard operating procedure (SOP) or policy.

f. Unit-oriented IO Checklist.

g. Self-inspection and inspection records -- maintain for three years.

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

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

j. Annual file review certification MFR -- maintain for three years.

ENCLOSURE J

COMPLIANCE INSPECTION GUIDANCE AND SELF-INSPECTION CHECKLISTS

1. NG units may be inspected by NGB, ARNG, major command, Service, and DoD SIOO inspectors.

a. Generally, the inspectors will request mission briefings from all intelligence and intelligence-related units and staffs in order 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 Books, and mandatory reference documents. They may ask to review intelligence files (hard and soft copy) to ensure no un-authorized 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 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 will provide a verbal out-brief upon completion of the inspection. Inspectors from the NGB and ARNG will follow up with a written report.

2. The NGB IG team will use reference k for inspections of NG JFHQs-State and unit T-32 IO programs.

3. DoD SIOO inspection checklists and other inspection information are available on the DoD SIOO websites, references bb and qq.

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 Policy or Continuity Book for a minimum of five years.

APPENDIX A TO ENCLOSURE J

PROCEDURE 1 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Is all intelligence or intelligence-related activity consistent with applicable Department of Defense, Service, and National Guard policy? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01C, para. 4, and Chief of the National Guard Bureau Manual [CNGBM] 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 1.b)	Yes or No
4. Do you host or participate in a shared repository?	Yes or No (If no, go to question 6.)
A. If you are a host, do you regularly audit access to U.S. person information (USPI) to the extent practicable? (CNGBM 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 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? (CNGBM 2000.01A, Enclosure A, para. 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. Is all information that you intentionally collect necessary for the performance of an authorized intelligence mission or function assigned to you? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01A, Enclosure A, para. 2.a)	Yes or No
2. Does all U.S. person information (USPI) that you intentionally collect fall into a category specified in CNGBM 2000.01A, Enclosure A, para. 2.a(1)-(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? (CNGBM 2000.01A, Enclosure A, para. 2.b(3))	Yes or No
4. Do you consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired and the intrusiveness of the collection methods? (CNGBM 2000.01A, Enclosure A, para. 2.c)	Yes or No
5. Do you notify the National Guard Bureau Joint Intelligence Directorate through the State Joint Intelligence Directorate in order to obtain authorization for special circumstances collections, notify the Department of Defense Senior Intelligence Oversight Official of the approval, and determine appropriate enhanced safeguards? (CNGBM 2000.01A, Enclosure A, para. 2.c.)	Yes or No
6. Do you collect information solely for the purpose of monitoring activities protected by the First Amendment or other Constitutional rights or U.S. law? (CNGBM 2000.01A, Enclosure A, para. 2.d(2))	Yes or No
7. Do you use the least intrusive collection technique feasible when collecting USPI? (CNGBM 2000.01A, Enclosure A, para. 2.d(3))	Yes or No
8. Do you, to the extent practicable, limit collection of non-publicly available information to no more information than is reasonably necessary? (CNGBM 2000.01A, Enclosure A, para. 2.d(3))	Yes or No
9. Do you have a process to ensure that collection of authorized USPI is done in accordance with this procedure? (CNGBM 2000.01A, Enclosure A, para. 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] 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 3.g)	Yes or No
4. Has National Guard Bureau Joint Intelligence Directorate or the State Joint Intelligence Directorate 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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.	

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 Department of Defense Senior Intelligence Oversight Official, a Component Inspector General, or the Attorney General. (CNGBM 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 3.k)	Yes or No
11. Do you review all electronic and hardcopy files at a minimum of once a 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 2000.01A, Enclosure A, para. 3.l)	Yes or No
12. Do you maintain on file for five 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 2000.01A, Enclosure A, para. 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] 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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
5. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 4.a(4)(b)?	Yes or No
6. Have you disseminated USPI to other Department of Defense elements? If no, proceed to question 8.	Yes or No
7. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 4.a(4)(c)?	Yes or No
8. Have you disseminated USPI to other Federal Government entities? If no, proceed to question 10.	Yes or No
9. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 4.a(4)(d)?	Yes or No
10. Have you disseminated USPI to State, local, tribal or Territorial governments?	Yes or No
11. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 4.a(4)(e)? If no, proceed to question 12.	Yes or No
12. Have you disseminated USPI to foreign governments? If so, has the dissemination to foreign governments or international organizations met the requirements in CNGBM 2000.01A, Enclosure A, para. 4.a(4)(f)?	Yes or No

Table 10. Procedure 4 Self-Inspection Checklist

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 the National Guard in carrying out an authorized mission or function? If you have not, proceed to question 15.	Yes or No
14. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 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? If no, proceed to question 17.	Yes or No
16. If so, has the dissemination met the requirements in CNGBM 2000.01A, Enclosure A, para. 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 National Guard Bureau Joint Intelligence Directorate or Vice Director of Joint Intelligence approve, after notifying the Department of Defense Senior Intelligence Oversight Official, the dissemination? (CNGBM 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 4.f)	Yes or No
19. Has any dissemination of USPI not conformed to the conditions set forth in Procedure 4 of CNGBM 2000.01A? If so, has the National Guard Bureau Joint Intelligence Directorate or the Vice Director of Joint Intelligence approved, on the advice of the National Guard Bureau Office of Chief Counsel after consultation with the General Counsel of the Department of Defense, the dissemination? (CNGBM 2000.01A, Enclosure A, para. 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 (FI) and counterintelligence purposes do so only while in a Title 10 status? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 5.b)	Yes or No
3. Are all requests to perform electronic surveillance, which includes computer network exploitation, for FI collection or against U.S. persons abroad for FI purposes, done so with the appropriate mission and authority? (CNGBM 2000.01A, Enclosure A, para. 5.c)	Yes or No
4. Do you ensure that SIGINT cryptologic element activities are conducted in accordance with applicable USSIDs? (CNGBM 2000.01A, Enclosure A, para. 5.d)	Yes or No
5. 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 2000.01A, Enclosure A, para. 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: 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

c. The use of TSCM has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken. d. If the use of TSCM constitutes electronic surveillance as that term is defined in the Foreign Intelligence Surveillance Act (FISA), such countermeasures are not targeted against the communications of any particular person or persons. (CNGBM 2000.01A, Enclosure A, para. 5.e(1))	Yes or No
7. National Guard Bureau Joint Intelligence Directorate (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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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, and time of activity) only in accordance with CNGBM 2000.01A, Enclosure A, para. 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] 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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, para 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, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 8.c)	Yes or No

Table 14. Procedure 8 Self-Inspection Checklist

Inspection Item	Yes or No
Do all National Guard Military Intelligence and counter-intelligence 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 2000.01A, Enclosure A, para. 9.b)	Yes or No

Table 15. Procedure 9 Self-Inspection Checklist

Inspection Item	Yes or No
Do all National Guard Military Intelligence and counter-intelligence 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 2000.01A, Enclosure A, para. 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 of Chief of the National Guard Bureau Manual 2000.01A, Enclosure A, para. 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] 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure A, para. 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 2000.01A, Enclosure E, para. 4.b)	Yes or No

4. Is all information under analysis 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 2000.01A, Enclosure A, para. 12.d)	Yes or No

Table 18. Procedure 12 Self-Inspection Checklist

Inspection Item	**Yes or No**
Do National Guard intelligence component elements engage in experimentation involving human subjects for intelligence purposes? (Chief of the National Guard Bureau Manual 2000.01A, Enclosure A, para. 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 law and applicable Department of Defense (DoD), Service, and National Guard Bureau policy? (Chief of the National Guard Bureau Manual [CNGBM] 2000.01A, Enclosure A, para. a, and Chief of the National Guard Bureau Instruction [CNGBI] 2000.01C, para. 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 2000.01C, para. 4.b.)	Yes or No
3. Do all National Guard (NG) personnel operating in a State active duty (SAD) status refrain from engaging in DoD intelligence and CI activities? (CNGBI 2000.01C, para. 4.d)	Yes or No
4. Do all NG personnel operating in a SAD 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 2000.01C, para. 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 2000.01C, para. 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 2000.01A, Enclosure A, para. b)	Yes or No
7. Is training documented and the documentation retained for five years?	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 2000.01A, Enclosure A, para. b)	Yes or No

Table 20. Employee Conduct Self-Inspection Checklist.

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

Table 20, continued. Employee Conduct Self-Inspection Checklist

APPENDIX H TO ENCLOSURE J

NATIONAL GUARD JFHQS-STATE J2 SELF-INSPECTION CHECKLIST

Inspection Item	**Yes or No**
1. Is the National Guard (NG) Joint Force Headquarters–State (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] 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 14.f)	Yes or No
8. Is training documented and the documentation retained for five 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 2000.01C, Enclosure A, para. 14.g)	Yes or No

Table 21. National Guard JFHQs-State J2 Self-Inspection Checklist

10. Is this training documented and the documentation retained for five years?	Yes or No
11. Has the J2, after consultation with the NG JFHQs-State JA, submitted proper use memorandums to the National Guard Bureau J2 for all domestic imagery training, exercises, or real-world missions flown in a Title 32 status? (CNGBI 2000.01C, Enclosure A, para. 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 reviews maintained on file in the IO Continuity Binder for five years? (CNGBI 2000.01C, Enclosure A, para. 14.l)	Yes or No
13. Does the 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 five years? (CNGBI 2000.01C, Enclosure A, para. 14.m)	Yes or No
14. Does the 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 2000.01C, Enclosure A, para. 14.n)	Yes or No

Table 21, continued. National Guard JFHQS-State J2 Self-Inspection Checklist

APPENDIX I TO ENCLOSURE J

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

Inspection Item	**Yes or No**
1. Is the commander, director, or senior intelligence officer (SIO) knowledgeable of the missions, plans, and capabilities of assigned and subordinate intelligence and intelligence-related capabilities and levying tasks and missions in accordance with intelligence oversight (IO) policy and guidance? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01C, Enclosure A, para. 17.b)	Yes or No
2. Has the commander, director, or SIO received initial and annual IO training? (CNGBI 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 17.e)	
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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 17.f)	Yes or No

Table 22. National Guard Commander, Director, and Senior Intelligence Officer 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 and/or NG JFHQs-State JA for review and submission to the National Guard Bureau Office of the Chief Counsel if required? (CNGBI 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 17.k)	Yes or No
13. Has the commander, director, or SIO submitted a quarterly IO report to the State Joint Intelligence Directorate? (CNGBI 2000.01C, Enclosure A, para. 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 Intelligence Oversight (IO) Monitor received initial and annual IO training? (Chief of the National Guard Bureau Instruction [CNGBI] 2000.01C, Enclosure A, para. 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 impacting their mission; reporting procedures for questionable intelligence activity, significant or highly sensitive matter, and Federal crimes; and the identity of the IO Monitors? (CNGBI 2000.01C, Enclosure A, para. 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 (IGs) in accordance with (IAW) Chief of the National Guard Bureau Manual [CNGBM] 2000.01A, Enclosure D? (CNGBI 2000.01, Enclosure A, para. 18.c)	
4. Has the IO Monitor maintained records for five calendar years, including the dates personnel received training, for all IO training? (CNGBI 2000.01C, Enclosure A, para. 18.c)	Yes or No
5. Has the IO Monitor maintained an IO Continuity Binder IAW CNGBM 2000.01A, Enclosure I? (CNGBI 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 18.f)	Yes or No

Table 23. NG 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 2000.01C, Enclosure A, para. 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 IAW Procedure 3 and certified that all files have been reviewed through a memorandum for record and maintained on file in the IO Continuity Book for five years? (CNGBI 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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? (CNGBI 2000.01C, Enclosure A, para. 18.j)	Yes or No

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

APPENDIX R 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] 2000.01C, Enclosure A, para. 19.a)	Yes or No
2. Are personnel familiar with the policies contained in CNGBI 2000.01C; 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 2000.01C, Enclosure A, para. 19.b)	Yes or No
3. Do personnel conduct intelligence and intelligence-related activities in accordance with applicable law and policy, including CNGBI 2000.01C and Manual 2000.01A and the policy of the appropriate intelligence discipline, and not exceed the authorities granted by them? (CNGBI 2000.01, Enclosure A, para. 19.c)	
4. Have personnel completed the organization's intelligence oversight (IO) training within 90 days of assignment or employment, as well as annual refresher training and pre-deployment IO training? (CNGBI 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 2000.01C, Enclosure A, para. 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 within one or more of the 13 authorized categories.

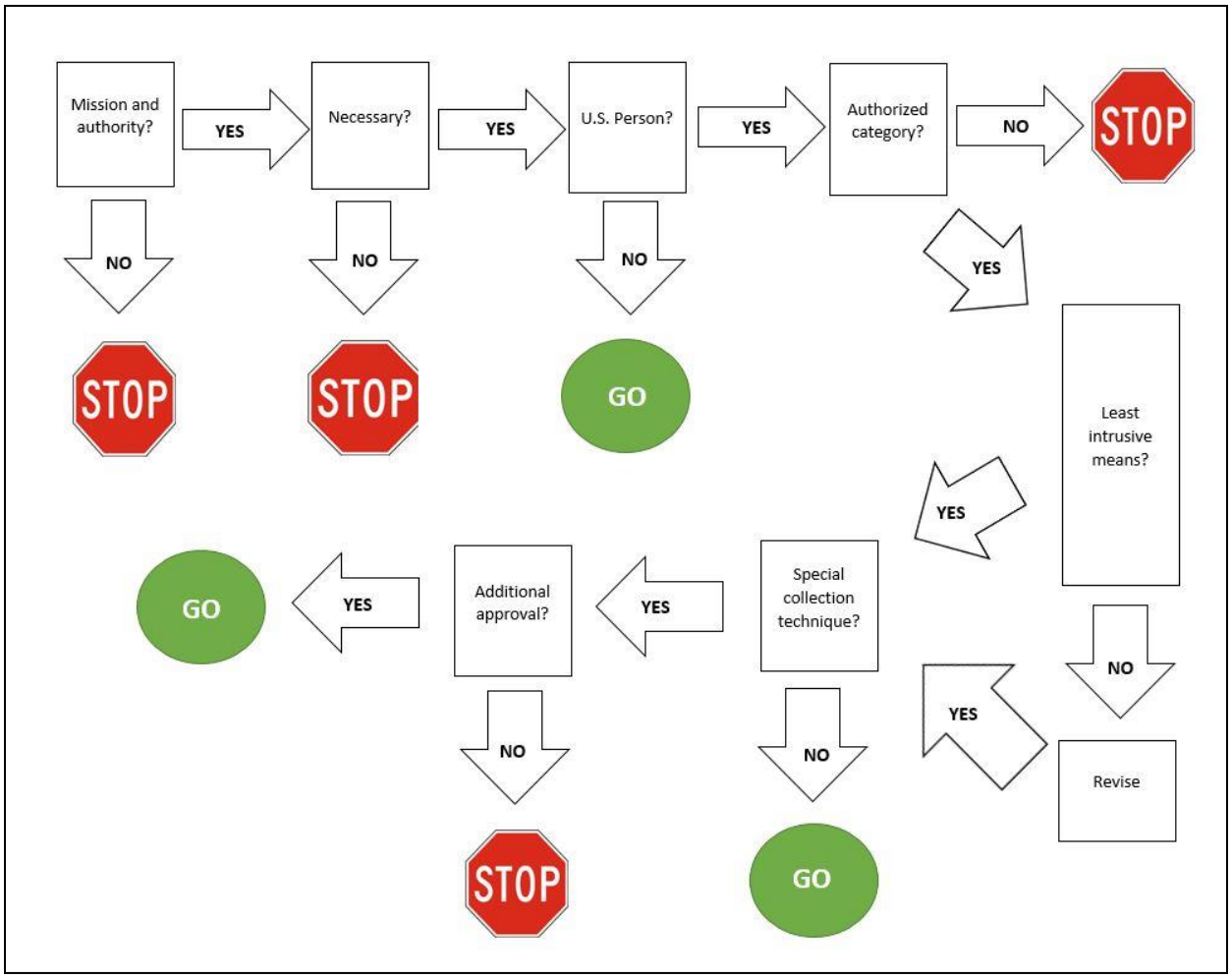

Figure 12. The Intelligence Oversight Process

2. Special collection techniques require additional approval. The flow chart in Figure 12 represents the decision-making process when considering how to handle USPI in the course of conducting NG intelligence and intelligence-related missions and functions.

3. Steps.

a. Step 1. Do you have the authority and mission to collect, process, analyze, retain, or disseminate the intelligence? If not, then stop; do not

collect, process, analyze, retain, or disseminate the intelligence. Your defined mission may be found in execute orders, operation orders, an EMAC, USSIDs, FEMA Mission Assignments, 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 not, then stop; do not collect, process, analyze, retain, or disseminate the intelligence.

c. Step 3. Is USPI involved? If not, 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 not, 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 not, 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 not, 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

a. CNGB Instruction 2000.01C, 14 August 2018, "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. DoD Directive 5148.13, 26 April 2017, "Intelligence Oversight"

d. DoD Directive 5240.01, 27 August 2007, "DoD Intelligence Activities," Incorporating Change 1 and Certified Current Through 27 August 2014

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

f. DoD 5240.1-R, December 1982, Incorporating Change 2, 26 April 2017, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons"

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 (AFI) 14-104, 05 November 2014, "Oversight of Intelligence Activities"

j. Air Force Guidance Memorandum to AFI 14-104, 04 October 2018, "Oversight of Intelligence Activities"

k. CNGB Instruction 0700.01, 21 December 2018, "Inspector General Intelligence Oversight"

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

m. U.S. 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 SE 3500 (ANG)(S), 11 January 2013

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

s. USD(I) Memorandum, 24 March 2014, "Request for Authority to Establish a Technical Surveillance Countermeasures Program (TSCM)"

t. DoD Manual S-5240.05, 23 April 2015, "(U) The Conduct of Technical Surveillance Countermeasures," Incorporating Change 1, 14 March 2016

u. Title 50 United States Code, Chapter 36, "The Foreign Intelligence Surveillance Act (FISA)"

v. 18 U.S. Code Chapter 119, "Wire and Electronic Communications Interception and Interception of Oral Communications"

w. 47 U.S. Code Section 605, "Unauthorized Publication or Use of Communications"

x. NGB J2 NIPRNET Intelligence Oversight Program website: https://gko.portal.ng.mil/joint/j2/J23/NG-J2_IO/default.aspx, 30 January 2019

y. Memorandum of Understanding Between the Attorney General and the Secretary of Defense, August 1995, "Reporting of Information Concerning Federal Crimes"

z. DoD Instruction 5240.04, 01 April 2016, "Counterintelligence (CI) Investigations," Incorporating Change 1, Effective 26 April 2018

aa. Constitution of the United States of America, 04 March 1789 (last amended 05 May 1992)

bb. DoD SIOO NIPRNET website: <https://dodsioo.defense.gov/Training/>, 30 January 2019

cc. 32 U.S. Code Section 112, "Drug Interdiction and Counter-drug Activities"

dd. CNGB Instruction 3100.01A, 22 June 2015, "National Guard Counterdrug Support"

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

ff. CNGB Instruction 2400.001A, 07 November 2013, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"

gg. Secretary of Defense Policy Memorandum, 21 August 2018, "Guidance for the Domestic Use of Unmanned Aircraft Systems in U.S. National Airspace"

hh. 10 U.S. Code Section 284, "Support for Counter-drug Activities and Activities to Counter Transnational Organized Crime"

ii. National System for Geospatial-Intelligence (NSG) Manual (NSGM) FA 1806, March 2009, "Domestic Imagery," Incorporating administrative update, May 2011

jj. NSG Policy Memorandum 1806, 05 July 2017, "Domestic Imagery"

kk. NSG Instruction 1806, 08 July 2017, "Interim Instruction Domestic Imagery"

ll. NSG Manual CS 9400.04, December 2009, "Commercial Remote Sensing Satellite Imagery Policy"

mm. CNGB Instruction 7500.00, 13 October 2016, "Domestic Use of National Guard Unmanned Aircraft Systems"

nn. DoD Instruction 8170.01, 31 December 2018, "Online Information Management and Electronic Messaging"

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

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

qq. DoD SIOO <SIPRNET: intellipedia.intelink.sgov.gov/wiki/Intelligence_Oversight_Inspections_and_Best_practices>, 30 January 2019

GLOSSARY

PART I. ACRONYMS

A2	Director of Intelligence (Air Force)
AFI	Air Force Instruction
ANG	Air National Guard
ARNG	Army National Guard
CBRNE	Chemical, biological, radiological, nuclear, and explosive
CD	Counterdrug
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
COCOM	Combatant command
COMSEC	Communications security
CRE	CBRNE Response Enterprise
DoD	Department of Defense
DoDM	Department of Defense Manual
EMAC	Emergency Management Assistance Compact
EO	Executive order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FI	Foreign intelligence
FISA	Foreign Intelligence Surveillance Act
FLIR	Forward-looking infrared radar
FOUO	For Official Use Only
FP	Force protection
G2	Director of Intelligence (Army)
GC	General Counsel
GEOINT	Geospatial intelligence
HD	Homeland defense
HUMINT	Human intelligence
IAA	Incident awareness and assessment
IAW	In accordance with
IG	Inspector General
IMINT	Imagery intelligence
IO	Intelligence oversight
IP	Internet Protocol
IR	Infrared
ISR	Intelligence, surveillance, and reconnaissance
J2	Joint Director of Intelligence
JA	Judge Advocate
LE	Law enforcement
LEA	Law enforcement agency
MASINT	Measurements and signatures intelligence

MEDINT	Medical intelligence
MFR	Memorandum for record
MI	Military Intelligence
NG	National Guard
NGA	National Geospatial-Intelligence Agency
NG JFHQs-State	National Guard Joint Force Headquarters–State
NGB	National Guard Bureau
NGB-JA	Office of the General Counsel
NSA	National Security Agency
OSINT	Open-source intelligence
PII	Personally identifiable information
PM	Provost Marshal
POC	Point of contact
PUM	Proper use memorandum
QIA	Questionable intelligence activity
RPA	Remotely piloted aircraft
S2	Intelligence Officer (Army)
SAD	State active duty
SAR	Search and rescue
SecDef	Secretary of Defense
S/HSM	Significant or highly sensitive matter
SIGINT	Signals intelligence
SIO	Senior intelligence officer
SIOO	Senior Intelligence Oversight Official
SIPRNET	Secret Internet Protocol Router Network
T-10	Title 10
T-32	Title 32
TAG	The Adjutant General
TDY	Temporary duty
TSCM	Technical surveillance countermeasures
UAS	Unmanned aircraft systems
UDP	Undisclosed participation
URL	Uniform Resource Locator
USD(I)	Under Secretary of Defense for Intelligence
USGS	United States Geological Survey
USPI	U.S. person information
USSID	United States Signals Intelligence Directive

PART II. DEFINITIONS

Air National Guard -- The organized militia of the States and Territories, Puerto Rico, 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 the Constitution; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference dd.

Army National Guard -- The organized militia of the States and Territories, Puerto Rico, 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 the Constitution; is organized, armed, and equipped wholly or partly at Federal expense; and is Federally recognized in accordance with reference dd.

Certifying National Guard 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 adviser to the Secretary of the Army, Secretary of the Air Force, Chief of Staff of the Army, and Chief of Staff of the Air Force on matters relating to Federalized forces of the National Guard of the United States and its subcomponents, the Army National Guard and Air National Guard of the United States.

Collection -- Receipt of information by a Defense Intelligence Component, whether 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 U.S. 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 mm, information compiled, analyzed, or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Criminal Investigation -- In accordance with reference nn, 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 Office of 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 Defense Agencies, the Department of Defense field activities, and all other organizational entities within the Department.

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 Executive Order 12333 applies.

Domestic Imagery -- Any imagery collected by satellite (national, tactical, or commercial) or airborne platforms that cover the land areas of the 50 States, the District of Columbia, and the Territories and possessions of the United States, to a 12-nautical-mile seaward limit of these land areas.

Domestic Imagery Request -- The request for collection, processing, dissemination, exploitation, briefing, or publication of domestic imagery when that need falls outside the scope of an approved proper use memorandum and is not a reflection of a change in the organization's mission. The request generally reflects ad hoc requirements for domestic imagery.

Eagle Vision -- A deployable ground station for processing imagery received directly from commercial satellite platforms.

E-mail Address -- An address that identifies a user so that the user can receive Internet e-mail. An e-mail 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 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; 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.

Federal Activity -- Any organizational unit of the Federal Government, including Federal departments, agencies, establishments, corporations (such as the Tennessee Valley Authority), boards, committees, commissions, councils, and quasi-official agencies (such as the Smithsonian Institution).

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 U.S. 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 the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

Homeland Defense -- The protection of U.S. sovereignty, territory, domestic population, and critical defense 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, and minimize the damage and recover from attacks that do 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.

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 (IP) 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 re-imbursable 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 ee. The Chief of the National Guard Bureau is under the authority, direction, and control of the Secretary of Defense.

National Guard Intelligence Component -- All National Guard Bureau personnel, National Guard Joint Force Headquarters–State personnel, Title 32 National Guard intelligence units and staff organizations, and Title 32 non-intelligence organizations that perform or train to perform intelligence or intelligence-related activities.

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.

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, the requirement that the function be both an authorized intelligence activity (foreign intelligence or counterintelligence) and a mission delegated to that specific Department of Defense intelligence component.

Non-United States Person -- A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States is not a U.S. person. A person or organization outside the United States. is presumed not to be a United Statesperson unless specific information to the contrary is obtained. An alien in the United States is presumed not to be a U.S. 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 (QIA)-- Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including references b and d, this manual, and/or other NGRs, Army and AF policy documents and instructions. Such a violation

is not a "questionable intelligence activity" in this context unless some connection exists between the activity and an intelligence function.

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 (CI) 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 CI work might not. Intelligence professionals should seek advice from intelligence oversight officer, chain of command, or trained JA for assistance in making determinations when necessary.

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 microblogging) 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 (URL) -- The URL is a standard way of specifying the location of an object on the Internet, typically a Web page. A URL represents an address used on the World Wide Web (www). Typically, URLs appear as words rather than numbers and, while some URLs 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 URL do not convey, in any apparent way, information concerning persons (or example, Bicyclists.com).

United States Person -- A United States citizen (born in the United States or naturalized), an alien known by the Department of Defense or National Guard intelligence component concerned to be a lawful permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States unless it is directed and controlled by a foreign government or governments.

United States Person Information (USPI) -- A U.S. 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 U.S. person. If several types of potentially identifying information exist about a U.S. person, which, when considered together, essentially identify the U.S. person, that collective information will be considered U.S. person identifying information. U.S. person information is either a single item or information combined with other items that 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. U.S. 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 U.S. person: name, e-mail address, address, phone number, IP address, Social Security number, physical description, driver's license number, date of birth, place of birth.

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.