



CHIEF NATIONAL GUARD BUREAU MANUAL

NGB-J2
DISTRIBUTION: A

CNGBM 2000.01
26 November 2012

NATIONAL GUARD INTELLIGENCE ACTIVITIES

Reference(s): See Enclosure S.

1. Purpose. This manual describes how to implement policies contained in Chief National Guard Bureau (CNGB) Instruction (I) (CNGBI) 2000.01, National Guard (NG) Intelligence Activities (reference a), and establishes procedures for the conduct and oversight of National Guard Bureau (NGB), Joint Forces Headquarters-State (JFHQ-S) and NG Title 32 (T-32) intelligence and intelligence-related activities. Procedures and information contained herein are in accordance with (IAW) references b, c, and d.
2. Superseded/Canceled. None.
3. Applicability. This manual applies to all NGB, T-32NG JFHQ-S, and T-32 NG intelligence units and staff organizations, and T-32 non-intelligence organizations that perform intelligence or intelligence-related activities, as defined in the glossary, hereinafter referred to as the NG intelligence component. This manual does not apply to criminal investigations or authorize any intelligence activity not otherwise authorized by law. NG members serving in a Title 10 (T-10) status must comply with Service Component regulations.
4. Procedures. References b and d give clear guidance for ensuring the legality and propriety of all intelligence and intelligence-related activity. The application of reference d to NG intelligence components is required by NG policy because it gives specific guidance for conducting this activity through 15 procedures. Procedure 1 provides general guidance. Procedures 2 through 4 articulate the exclusive procedures through which Department of Defense (DoD) intelligence components, which includes the NG intelligence component IAW this manual, may collect, process, retain, and disseminate information concerning United States (U.S.) persons. Procedures 5 through 10 define

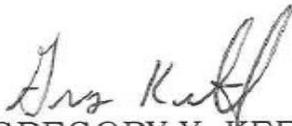
UNCLASSIFIED

procedures regarding the use of special collection techniques used to obtain information for foreign intelligence (FI) and counterintelligence (CI) purposes. Authority to employ these techniques is limited to that necessary to perform functions assigned to the DoD intelligence component concerned. Procedures 11 through 13 regulate other aspects of DoD intelligence activities, including oversight of those activities. Procedure 14 governs the training and official conduct of intelligence professionals and non-intelligence personnel engaged in intelligence and intelligence-related activities. Procedure 15 defines the requirement to report and investigate misconduct incident to intelligence and intelligence-related activities that violates the laws, policies, or regulations governing those activities. Specific procedural guidance is contained in Enclosure A.

5. Summary of Changes. This is the initial publication of CNGBM 2000.01.

6. Releasability. This manual is approved for public release; distribution is unlimited. NGB directorates, the Adjutants General (TAGs), the Commanding General of the District of Columbia, and NG JFHQ-S may obtain copies of this manual through www.ngbpd.c.ngb.army.mil.

7. Effective Date. This manual is effective upon publication.


GREGORY Y. KEETCH
Colonel, USAF
Director, Joint Intelligence

Enclosures:

- A -- Procedural Guidance
- B -- National Guard Intelligence and Counterintelligence Missions
- C -- Intelligence Oversight Training Requirements
- D -- Domestic Operations
- E -- Domestic Imagery
- F -- Proper Use Memorandum Format
- G -- Amended Proper Use Memorandum Format
- H -- Private Corporation Letter of Consent Format
- I -- Private Individual Letter of Consent Format
- J -- Procedure 12 Memorandum Format
- K -- Intelligence Support to Force Protection
- L -- Multi-National and State Partnership Program Intelligence

Activities

- M -- Computer Networks
- N -- The Intelligence Oversight Continuity Binder
- O -- Compliance Inspection Guidance
- P -- The Intelligence Oversight Process
- Q -- Sample Intelligence Oversight Wallet Card
- R -- References
- GL -- Glossary

TABLE OF CONTENTS

PART	Page
Purpose	1
Superseded/Canceled	1
Applicability	1
Procedures	1
Summary of Changes	2
Releasability	2
Effective Date	2
ENCLOSURE A -- PROCEDURAL GUIDANCE	A-1
Procedure 1: General	A-1
Procedure 2: Collection	A-1
Procedure 3: Retention	A-7
Procedure 4: Dissemination	A-9
Procedure 5: Electronic Surveillance	A-10
Procedure 6: Concealed Monitoring	A-11
Procedure 7: Physical Searches	A-12
Procedure 8: Searches and Examination of Mail	A-12
Procedure 9: Physical Surveillance	A-13
Procedure 10: Undisclosed Participation in Organizations	A-14
Procedure 11: Contracting for Goods and Services	A-17
Procedure 12: Provision of Assistance to Law Enforcement Authorities	A-17
Procedure 13: Experimentation on Human Subjects for Intelligence Purposes	A-20
Procedure 14: Employee Conduct	A-20
Procedure 15: Identifying, Investigating, and Reporting Questionable Intelligence Activity, Significant or Highly Sensitive Matters, and Crimes Reported to the Attorney General	A-21
ENCLOSURE B -- NATIONAL GUARD INTELLIGENCE AND COUNTERINTELLIGENCE MISSIONS	B-1
Introduction	B-1
Geospatial Intelligence/Imagery Intelligence	B-1
Signals Intelligence	B-1
Human Intelligence	B-1
Open-Source Intelligence	B-2
Measurements and Signatures Intelligence	B-2
Medical Intelligence	B-2
Counterintelligence	B-3

ENCLOSURE C – INTELLIGENCE OVERSIGHT TRAINING REQUIREMENTS	C-1
Training Requirements	C-1
Initial Training.....	C-1
Annual Refresher Training.....	C-1
Pre-deployment/Temporary Duty Training.....	C-2
Training Development	C-2
Training Records	C-4
Additional Training Requirements for SIGINT Units	C-4
ENCLOSURE D -- DOMESTIC OPERATIONS	D-1
Homeland Defense	D-1
Homeland Security.....	D-1
Defense Support of Civilian Authorities Intelligence Activities	D-1
General Information.....	D-1
Search and Rescue	D-2
Incident Awareness and Assessment.....	D-2
National Guard Baseline Operating Posture.....	D-3
ENCLOSURE E -- DOMESTIC IMAGERY	E-1
General	E-1
Domestic Imagery from National Satellites.....	E-2
Domestic Imagery from Airborne Platforms.....	E-2
Domestic Imagery from Commercial Satellites	E-2
Fighter, Bomber, Remotely Piloted Aircraft, Unmanned Aircraft System, and Unmanned Aerial Vehicle Navigational/Target Training Activities	E-3
Proper Use Memorandums and Proper Use Memorandums for Record ..	E-3
Immediate Approval Authority	E-8
Dissemination of Domestic Imagery	E-9
Analysis of Domestic Imagery	E-10
ENCLOSURE F -- PROPER USE MEMORANDUM FORMAT	F-1
ENCLOSURE G -- AMENDED PROPER USE MEMORANDUM FORMAT.....	G-1
ENCLOSURE H -- PRIVATE CORPORATION LETTER OF CONSENT FORMAT	H-1
ENCLOSURE I -- PRIVATE INDIVIDUAL LETTER OF CONSENT FORMAT	I-1

ENCLOSURE J -- PROCEDURE 12 MEMORANDUM FORMAT.....	J-1
ENCLOSURE K -- INTELLIGENCE SUPPORT TO FORCE PROTECTION	K-1
General	K-1
Dual-Hatting of Intelligence, AT/FP, and/or PM Personnel	K-3
Reporting Incidentally Acquired Threat Information	K-3
ENCLOSURE L -- MULTI-NATIONAL AND STATE PARTNERSHIP PROGRAM INTELLIGENCE ACTIVITIES	L-1
ENCLOSURE M -- COMPUTER NETWORKS	M-1
General	M-1
Internet Protocol Addresses	M-1
E-mail Addresses	M-2
Uniform Resource Locators.....	M-3
ENCLOSURE N -- THE INTELLIGENCE OVERSIGHT CONTINUITY BINDER.....	N-1
ENCLOSURE O -- COMPLIANCE INSPECTION GUIDANCE.....	O-1
ENCLOSURE P -- THE INTELLIGENCE OVERSIGHT PROCESS.....	P-1
ENCLOSURE Q -- SAMPLE INTELLIGENCE OVERSIGHT WALLET CARD..	Q-1
ENCLOSURE R -- REFERENCES.....	R-1
GLOSSARY	GL-1
FIGURES	
1. Intrusive Means of Collection Scale.....	A-8
2. Is a PUM Required?.....	E-7
3. Sensitive Information Handling.....	K-2
4. The Intelligence Oversight Process	P-1
TABLES	
1. Categories of U.S. Persons Information	A-5
2. Examples of U.S. Persons Identifying Data	A-7

ENCLOSURE A

PROCEDURAL GUIDANCE

1. **Procedure 1.** General.

a. All NG personnel will conduct intelligence and intelligence-related activities only pursuant to and IAW references a, b, c, d, e, and f and this manual; personnel will not exceed the authorities granted by these references or by applicable laws, executive orders (EOs), regulations, instructions, or policies.

b. The procedures set forth in reference d do not apply to law enforcement (LE) or civil disturbance activities, activities related to the restoration of order, or activities associated with responses to natural disasters involving humanitarian assistance undertaken by NG intelligence components when directed by the Secretary of Defense (SecDef) or his or her designated representative. These activities include, but are not limited to: reconnaissance missions for damage assessment; route analysis and infrastructure studies; support of response to chemical, biological, radiological, nuclear, and explosive (CBRNE) incidents; hydrographic surveys; and search and rescue (SAR) operations.

c. For the purposes of this manual, a U.S. person is defined as a U.S. citizen (born in the U.S. or naturalized), an individual known by the NG intelligence component to be a lawful permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a U.S. corporation unless it is directed and controlled by one or more foreign governments.

2. **Procedure 2.** Collection.

a. Least intrusive means. NG intelligence components may collect U.S. persons' information by the least intrusive means possible if the intelligence component has the authorized mission and 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 following 15 categories of information:

(1) Information obtained with consent. Information may be collected about U.S. persons who consent to such collection (e.g., a JFHQ-S Joint Director of Intelligence (J2) collects imagery of a privately owned power plant with the consent of the owner for Joint Intelligence Preparation of the Operational Environment (JIPOE) purposes).

(2) Publicly available information. NG intelligence components may collect information about U.S. persons if it is publicly available (e.g., on the Internet or in a published document) and necessary to an assigned mission or function (e.g., a JFHQ-S J2 collects information detailing emergency exits and the number of beds in local hospitals from public records).

(3) FI. Subject to the special limitations contained in paragraph 3.f.(2) below, intentional collection of U.S. persons information because the information constitutes FI is permitted if the U.S. person meets one of the following descriptions:

(a) Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf of a foreign power.

(b) An organization or entity reasonably believed to be owned or controlled, directly or indirectly, by a foreign power.

(c) Persons or organizations reasonably believed to be engaged in or about to engage in international terrorism or international narcotics activities.

(d) Persons who are reasonably believed to be prisoners of war, missing in action, or are the targets, hostages, or victims of international terrorists or terrorist organizations.

(e) Persons or entities reasonably believed to be engaged in or about to engage in attacks or intrusions into DoD information systems; DoD contractor information systems that impact DoD personnel, property, or missions; or U.S. Government national security systems on behalf of a foreign power, international terrorist, or international terrorist organization.

(f) Persons or entities reasonably believed to be engaged or about to engage in the targeting, exploitation, or illegal diversion of DoD military and related technology on behalf of a foreign power.

(g) Individuals in contact with persons or entities described in paragraphs 3.a.(3)(a) through (f) above for the purpose of identifying such persons and assessing their relationship with persons described therein.

(h) Corporations or other commercial organizations reasonably believed to have some relationship with foreign powers, organizations, or persons.

(4) CI. U.S. persons information may be collected if it constitutes CI. Intentional collection of U.S. persons information for CI purposes is limited to the following:

(a) Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power or international terrorist.

(b) Persons in contact with those described in paragraph 3.a.(3)(a) above, for the purpose of identifying such persons and assessing their relationship with each other.

(5) Information obtained in the course of properly authorized investigative activities. U.S. persons information may be collected if the information was obtained in the course of any properly authorized investigative activity even if the U.S. person is not the target of the investigation. Such activities include, but are not limited to, CI investigations or inquiries, international narcotics or international terrorist investigations, administrative investigations, or commander inquiries.

(6) Potential sources of assistance to intelligence activities. Information on U.S. persons reasonably believed to be potential intelligence sources, or potential sources of assistance to intelligence activities may be collected so the intelligence component may assess their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

(7) Persons in contact with sources or potential sources. U.S. persons information may be collected for the purpose of assessing their relationship with a source or potential source.

(8) Protection of intelligence sources and methods. Information may be collected about a U.S. person who has or had access to or possession of information revealing FI and CI sources or methods, when the collection is necessary to protect against the unauthorized disclosure of that information. Within the U.S., collection is limited to the following:

(a) Present and former DoD employees.

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

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

(9) Physical Security. Information may be collected about a U.S. person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. A collecting component that comes into possession of information that fits this category, but does not have the assigned mission, has the obligation to pass the information immediately IAW applicable controls on dissemination of U.S. persons information to an organization with the mission to ensure the physical security of DoD personnel, installations, operations, or official visitors.

(10) Personnel Security. Information may be collected about U.S. persons arising from a lawful personnel security investigation. The collecting component must have been or be supporting a legitimately assigned personnel security mission and must be able to articulate both the discernable foreign connection of the U.S. persons who are the collection targets and the personnel security threat they pose.

(11) Communications Security (COMSEC). The NG intelligence component may collect U.S. persons' information during a lawful COMSEC inquiry or investigation. However, the collecting component must have been or be supporting a legitimately assigned mission to investigate COMSEC violations and must be able to articulate both the discernable foreign connection of the U.S. persons who are the collection targets and the COMSEC threat they pose.

(12) Threats to safety. U.S. persons' information may be collected to protect the safety of any person or organization, including those who are victims, targets, or hostages of international terrorist organizations or individuals. An NG intelligence component that comes into possession of information that fits this category, but does not meet its assigned mission, has the obligation to pass the information immediately IAW applicable controls on dissemination of U.S. persons information to an organization with the mission to ensure the safety of the persons or organizations concerned. U.S. persons who are known to be victims, targets, or hostages of an international terrorist organization or individual are presumed to have a foreign connection.

(13) Overhead and airborne reconnaissance. Information may be collected from overhead and airborne reconnaissance not directed at specific U.S. persons or from efforts directed at specific U.S. persons IAW applicable statutes, EOs, regulations, instructions, and the requirements in Enclosure D.

(14) Incidentally acquired information. Information obtained incidental to authorized intelligence collection activities may be collected if it qualifies for collection under any provision of this procedure, or if it indicates involvement in activities that may violate federal, state, local, or foreign laws.

(15) Administrative purposes. U.S. persons information that is necessary for administrative purposes (e.g., addresses and phone numbers for recall rosters) may be collected.

b. A U.S. person is identified when his or her name, nickname, alias, unique title, Social Security number, or other unique personal identifier is revealed. 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 that, when

considered together, essentially identify the U.S. person, then that collective information will be considered U.S. persons identifying information.

U.S. persons information may be collected by the least intrusive means possible if the intelligence component has the authorized mission or function to collect the information and the information is necessary to accomplish the authorized mission or function and the information falls within one or more of the following 15 categories:

- | | |
|--|---|
| 1. Information obtained with consent | 8. Protection of intelligence sources and methods |
| 2. Publicly available information | |
| 3. Foreign intelligence | 9. Physical security |
| 4. Counterintelligence | 10. Personnel security |
| 5. Obtained in the course of properly conducted investigative activities | 11. Communications security |
| 6. Potential sources of assistance to intelligence activities | 12. Threats to safety |
| 7. Persons in contact with sources or potential sources | 13. Overhead and airborne reconnaissance |
| | 14. Incidentally acquired information |
| | 15. Administrative purposes |

Table 1. Categories of U.S. Persons Information

c. Information is considered “collected” only when it has been received for use by an employee of an intelligence component in the course of official duties and affirmative action is taken that shows intent to use or retain that information. Data acquired by electronic means is “collected” only when it has been processed into intelligible form. NG intelligence personnel may receive information from anyone, at any time, to determine its intelligence value and whether it can be collected, retained, and/or disseminated.

d. Information received about U.S. persons may be kept temporarily, for a period not to exceed 90 days, solely for the purpose of determining if that information may be collected under the provisions of Procedure 2, and permanently retained under the provisions of Procedure 3. If the receiving organization is uncertain if the U.S. persons information may be collected and permanently retained, then it should seek advice through the chain of command. The organization Intelligence Oversight (IO) monitor, senior intelligence officer (SIO), Judge Advocate (JA), and/or Inspector General (IG) must assist in collectability determinations. When appropriate, the receiving organization may request assistance from NGB-J2. In no event may a determination take longer than a total of 90 days.

e. If it is determined that the information is not properly collectible before the expiration of the 90-day period, then it must immediately be redacted, purged, or transferred. Information considered uncollectible may be retained as long as necessary to transfer it to another DoD entity or government agency to whose function it pertains, but no longer.

f. Means of collection. When NG intelligence components are authorized to collect information about U.S. persons, they may do so by any lawful means, provided that all such collection activities are carried out IAW references b and d, and this manual, subject to the following limitations:

(1) Least intrusive means. Collection of information about U.S. persons will be accomplished by the least intrusive means possible. In general, this means:

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

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

(c) If collection from cooperating sources is not feasible or sufficient, then 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 (AG).

(d) If other lawful intelligence collection techniques that do not require a judicial warrant or the approval of the U.S. AG are not feasible or sufficient, then approval may be sought through the NGB-J2, to use intelligence collection techniques that require a judicial warrant or approval from the U.S. AG.

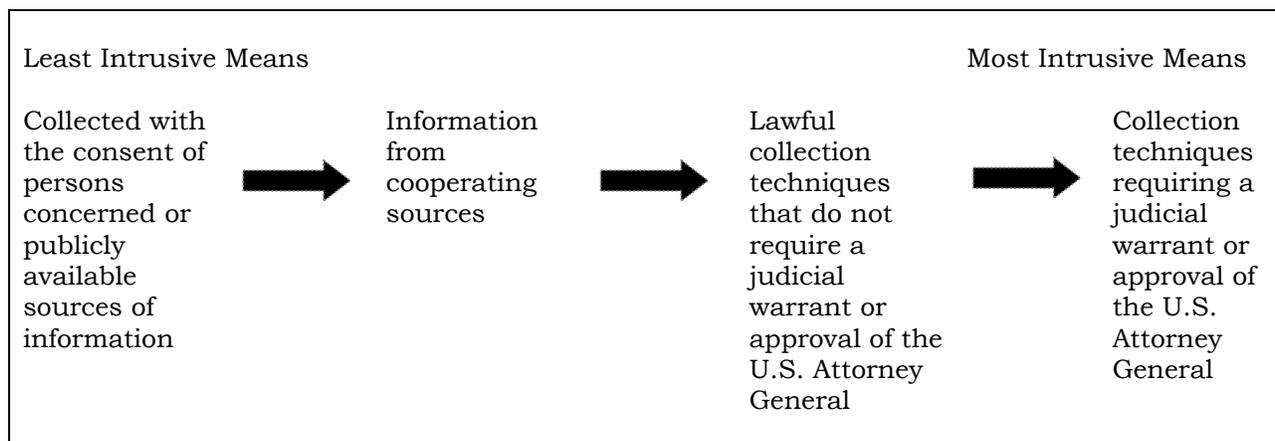


Figure 1. Intrusive Means of Collection Scale

(2) FI collection within the U.S. Within the U.S., FI concerning U.S. persons may be collected only by overt means except as provided below. Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that the information is being

provided to the intelligence component. Collection by other than overt means may be allowed if all of the following criteria are satisfied:

(a) The FI sought must be 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 by overt means.

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

(d) The use of any means other than overt has been approved by the appropriate authority. A copy of any approval granted IAW this procedure shall be provided through NGB-J2 to the Under Secretary of Defense, Intelligence (USD (I)).

3. **Procedure 3.** Retention.

a. Retention limitations apply to U.S. persons information that is knowingly retained without the consent of the person to whom the information pertains. These limitations do not apply to information retained solely for administrative purposes or information that is required to be retained by law. "Retention" refers only to the maintenance of information about U.S. persons that can be retrieved by reference to an individual's name or other identifying data (e.g., Social Security number). If an additional step is required to attach a piece of information that identifies someone, then it is not considered a U.S. persons information.

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 U.S. Persons Identifying Data

b. U.S. persons information may be retained under the following criteria:

(1) The information was properly collected IAW Procedure 2.

(2) The information was incidentally acquired and one of the following applies.

- (a) It could have been collected intentionally IAW Procedure 2.
- (b) It is necessary to understand or assess FI or CI.
- (c) It is FI or CI collected from authorized electronic surveillance.

(d) It indicates involvement in activities that may violate federal, state, local, or foreign law. Unless otherwise suitable for retention for reasons listed above, such information may be retained only as long as required to be disseminated to an appropriate LE or antiterrorism (AT)/force protection (FP) activity IAW Procedure 4.

(3) Information related to functions of other NG activities, DoD components, or non-DoD agencies. The information pertains solely to the functions and responsibilities of other activities, components, or agencies, and is retained only as necessary to transmit the information to that agency.

(4) Temporary retention. Information may be retained up to 90 days, solely to determine if the information is retainable under this instruction. The 90-day period starts upon receipt of the information. Discovery of additional significant information providing further indication of a foreign connection may provide a basis for restarting the temporary 90-day retention period.

(5) Other information. Information not covered in this section is retained only to report the collection for oversight purposes and for necessary subsequent processing.

c. Access and retention.

(1) Access to U.S. persons information is limited to those with a need to know.

(2) NG intelligence components will establish internal procedures for documenting decisions to retain U.S. persons information.

(3) Intelligence files and documents that contain information specifically identifying any U.S. person, whether retained in print or electronic format, or posted to an Internet website, must contain the following U.S. persons warning notice:

“ATTENTION: This document contains U.S. persons information, which has been included consistent with all applicable laws, directives, and policies.”

This requirement applies whether or not the U.S. person is the subject of the collected information. In the case of electronic files, this requirement may

be satisfied with an access banner identifying that users may encounter U.S. persons' information. Individual intelligence products must be marked appropriately. NG intelligence components must determine if it is appropriate for intelligence products posted to the Internet for general access to contain specific U.S. persons information. If the determination is made to minimize or redact such information, then the product posted should clearly indicate how that U.S. persons information may be attained should a mission require it.

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

(b) The first time a U.S. person appears in a document, the marking "USPER" will precede the name and/or alias. This designator will only be used the first time the name of the U.S. person appears in the product.

(4) NG intelligence components will review all electronic and hard copy files at a minimum of once a calendar year to ensure retention of U.S. persons information is still necessary to an authorized function, has not been held beyond established disposition criteria, and was not retained in violation of reference d. A letter certifying the review was conducted and no unauthorized U.S. persons information has been retained will be maintained on file in the IO Continuity Binder.

4. **Procedure 4.** Dissemination.

a. U.S. persons information in the possession of an NG intelligence component may be disseminated without the consent of the U.S. person pursuant to law, court order, or IAW the following criteria:

(1) The information was properly collected and/or retained IAW Procedures 2 and 3.

(2) The recipient is reasonably perceived to have a legitimate need to receive the information for the performance of a lawful governmental function and is:

(a) An employee of the DoD or an employee of a DoD contractor who has a need for such information in the course of his or her official duties.

(b) A federal, state, or local government LE entity, and the information indicates involvement in activities that may violate laws that the recipient is responsible to enforce.

(c) An agency within the U.S. Intelligence Community (IC). The agency concerned determines whether the information is relevant to the responsibilities of any such intelligence agency.

(d) An agency of the federal government authorized to receive such information in its performance of a lawful governmental function.

(e) A foreign government where dissemination is undertaken pursuant to an agreement or other understanding, or when the U.S. government is authorized to share such information in the performance of a lawful governmental function IAW applicable foreign disclosure law, policy, and guidance.

b. Dissemination criteria applies equally to physical and electronic files and databases to which a collecting intelligence component may allow access by personnel outside of its organization, to include posting information or documents to websites. It does not apply to information collected solely for administrative purposes.

c. Any dissemination that does not conform to the conditions set forth in this paragraph must be approved by NGB-JA through NGB-J2. Such a determination will be based on a conclusion that the proposed dissemination complies with applicable laws, EOs, and regulations.

5. **Procedure 5.** Electronic Surveillance.

a. NG intelligence components with the mission and authority may conduct electronic surveillance for FI and CI purposes only while in a T-10 status or while performing duties in a T-32 status under the oversight of a T-10 authority.

b. Electronic surveillance for CI purposes must be conducted IAW regulations, instructions, and procedures approved by the Secretary of the Army (for Army National Guard (ARNG)) or Secretary of the Air Force (AF) (for Air National Guard (ANG)), and contained in U.S. Signals Intelligence (SIGINT) directives (USSIDs), including reference g.

c. The Director of Intelligence for the Army (G2) or the Air Force (A2) must approve requests to perform electronic surveillance, which includes computer network exploitation, for FI collection or against U.S. persons abroad for FI purposes, even if the surveillance is consensual. Submit requests to the Department of the Army Deputy Chief of Staff (DCS) for Intelligence [DCS, G2 (DAMI-CDC) (ARNG)] or the AF DCS for Intelligence, Surveillance, and Reconnaissance [(AF/A2) (ANG)] through NGB-J2 for approval and coordination.

d. Commands that have SIGINT cryptologic elements will ensure that those elements conduct activities IAW applicable USSIDs, such as reference h or i.

6. **Procedure 6**. Concealed Monitoring.

a. Monitoring of individuals for LE purposes within the U.S. and of U.S. persons outside the U.S., where no reasonable expectation of privacy exists and no warrant is required, requires approval by at least one of the following four offices: the DCS, G-2, the Commander, U.S. Army Intelligence and Security Command (INSCOM) (Army FI and CI), the AF/A2 after consultation with the Secretary of AF Deputy General Counsel for National Security and Military Affairs [(SAF/GCM) (AF FI)], or the Commander, Air Force Office of Special Investigations (AFOSI) after consultation with AFOSI/JA (AF CI).

Within the U.S., when the subject has a reasonable expectation of privacy and a warrant would be required for LE purposes, treat and process concealed monitoring as electronic surveillance. Monitoring is considered to be within the U.S. if the monitoring device, or the monitored target, is located within the U.S.

b. Approval officials must determine that such monitoring is necessary to the conduct of assigned FI or CI functions and does not constitute electronic surveillance.

c. Within the U.S., an NG intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by DoD, or otherwise in the course of a CI investigation pursuant to the agreement governing the conduct of DoD CI activities in conjunction with the reference j.

d. When determining if concealed monitoring is appropriate, the following will be examined:

(1) Purpose. The monitoring is necessary for assigned FI or CI functions and does not constitute electronic surveillance.

(2) Definition. Concealed monitoring is the targeting, by electronic, optical, or mechanical means, of movements and activity of an individual or group.

(3) Electronic means. Electronic means include transponders, beepers, Global Positioning System (GPS) locators, and other approved technology for observing or tracking people.

(4) Optical means. Optical means include cameras and lenses of any type.

(5) Mechanical means. Mechanical means are devices that are neither electronic nor optical.

(6) Same or similar techniques. The same or similar techniques are often used for electronic surveillance. Careful review is necessary during the approval process to ensure that Procedure 5 does not apply.

7. **Procedure 7.** Physical Searches.

a. A physical search is any intrusion upon a person or a person's property or possessions to obtain property or information. Examination of areas in plain view and visible to the naked eye, if no physical trespass is required, or of items that are abandoned in a public place, does not constitute a physical search. Physical searches upon entering military installations and restricted areas on such installations are not covered under this provision because entrance constitutes consent. Nor does any intrusion authorized as necessary to accomplish lawful electronic surveillance constitute a physical search.

b. Physical searches within the U.S. ARNG CI elements are authorized to conduct nonconsensual searches in the U.S. for CI purposes of the person or property of active duty military personnel in a T-10 or T-32 status under a T-10 authority. This may be authorized by a military judge or magistrate, or a military commander empowered to approve physical searches for LE purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers. ARNG CI elements may not otherwise conduct nonconsensual physical searches within the U.S. for FI or CI purposes. The FBI is the lead agency to conduct any other nonconsensual search for FI or CI purposes.

c. Physical searches outside the U.S. ARNG CI activity performed outside the U.S. must be conducted in T-10 status IAW Service policies.

8. **Procedure 8.** Searches and examination of mail.

a. Procedure 8 applies to mail covers and the opening of mail within U.S. postal channels for FI and CI purposes. It also applies to the opening of mail to or from U.S. persons where the mail is not in U.S. postal channels and the mail opening occurs outside the U.S. Procedure 8 does not apply to searches of incoming and outgoing first-class mail at DoD incarceration facilities when authorized by their policies.

b. Applicable postal regulations do not permit NG intelligence elements to detain or open first-class mail within U.S. postal channels for FI or for CI purposes, nor to request that the U.S. Postal Service (USPS) take such action on their behalf. Searches of first-class mail in U.S. military postal channels overseas may only be authorized under procedures established in reference k, chapter 10.

c. NG intelligence components may request that appropriate U.S. postal authorities inspect, or authorize the inspection of second, third, or fourth-class mail in U.S. postal channels IAW applicable postal regulations. Such components may also request that U.S. postal authorities detain, or permit detention of, mail that may become subject to search under applicable postal regulations.

d. NG intelligence components may open mail to or from a U.S. person that is found outside U.S. postal channels only with the approval of the U.S. AG. Any requests for such authorization will be forwarded through NGB-J2 to (Army) the Office of the DCS, G2 (DAMI-CDC) or (AF) AF/A2.

e. Mail outside U.S. postal channels when both the sender and intended recipient are not U.S. persons, may be searched if such search is otherwise lawful and consistent with any applicable Status of Forces Agreements (SOFAs). Any requests for such authorization will be forwarded through command channels to (Army) the Office of the DCS, G2 (DAMI-CDC) or (AF) AF/A2.

9. **Procedure 9**. Physical Surveillance.

a. General.

(1) Procedure 9 applies to nonconsensual physical surveillance for FI or CI purposes. It does not apply to physical surveillance conducted as part of a training exercise in which the surveillance subjects are exercise participants. It also does not apply to counter-surveillance, where NG military intelligence (MI) personnel must detect foreign physical surveillance.

(2) Physical surveillance includes a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present threat through any means not involving electronic surveillance. Any physical surveillance that occurs outside a DoD installation shall be coordinated with the FBI (within the U.S.), Central Intelligence Agency (CIA) (outside the U.S.), or other agency as appropriate through established procedures.

b. Physical surveillance of U.S. persons within the U.S.

(1) NG MI personnel. Within the U.S., given the mission, authority, and necessity, NG MI personnel may conduct nonconsensual physical surveillance of U.S. persons who fall into the following categories:

(a) Military personnel on active duty status.

(b) Present or former intelligence component employees.

(c) Present or former intelligence component contractors and their present or former employees.

(d) Applicants for intelligence component employment or contracting.

(e) Persons in contact with those who fall into categories (a) to (d) above, to the extent necessary to identify the individual in person.

(2) NG CI components. NG CI components may assist the FBI in conducting physical surveillance of U.S. persons, both on and off a DoD installation at the request of the FBI IAW reference 1 and Army or AF CI policy. When outside a DoD installation, NG CI components may assist the FBI when a specific threat to DoD exists. Such surveillance may be approved through appropriate channels.

c. Physical surveillance of non-U.S. persons within the U.S.

(1) Physical surveillance of non-U.S. persons for any lawful function assigned an MI element must be approved through command channels.

(2) Surveillance outside a DoD installation within the U.S. must be coordinated with the FBI and other law enforcement agencies (LEAs), as appropriate.

10. **Procedure 10.** Undisclosed participation in organizations.

a. Undisclosed participation in organizations. This procedure applies to NG intelligence component personnel participating in any organization within the U.S., or a U.S. persons' organization outside the U.S., on behalf of the intelligence component. It will also apply when an employee is asked to take action within an organization for the intelligence component benefit, whether the employee is already a member or is asked to join an organization. Actions for intelligence component benefit will include collecting information, identifying potential sources or contacts, and other activities directly relating to FI or CI functions. It will not apply to:

(1) Participation for purely personal reasons if undertaken at the intelligence component employee's initiative and expense, and for personal benefit.

(2) NG intelligence component personnel attending training programs for non-intelligence purposes (e.g., leadership/management development and other training common to all military organizations).

(3) Cooperating sources who volunteer information obtained as a result of their participation in an organization. Information is volunteered when the source was not given prior direction or tasking to collect the information.

b. Criteria. Except as authorized below, NG intelligence component personnel may participate in organizations on behalf of the intelligence component only if their intelligence component affiliation is disclosed to an appropriate organization official, such as an organization executive officer or an official in charge of membership, attendance, or organizational records. Undisclosed participation must:

(1) Be essential to achieving a lawful FI or CI purpose within the unit assigned mission, with prior approval through the command chain.

(2) Not be conducted within the U.S. to collect FI from or about a U.S. person, or to collect information to assess a U.S. person as a potential source of assistance to FI activities. This does not preclude collecting information volunteered by cooperating sources within the organization, if otherwise permitted by Procedure 2 of this manual.

(3) Not include collection about the domestic activities of the organization or its members.

(4) Last no longer than 12 months, unless an appropriate official re-approves participation. The approving authority will place the original signature approval document permanently in the file or dossier. Further dissemination is not required unless required by law or competent authority.

(5) Not be conducted for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not U.S. persons and are reasonably believed to be acting on behalf of a foreign power. Any requests for such participation will be forwarded through command channels to (Army) DCS, G2 (DAMI-CDC) or (AF) AF/A2.

c. Participation types.

(1) General participation. General participation includes:

(a) Meetings open to the public, including professional seminars or conferences open to members of a particular profession, whether or not they are members or received a special invitation.

(b) Organizations that permit U.S. government employees to participate.

(c) Educational or professional organizations to enhance employee professional skills, knowledge, or capabilities.

(d) Seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar meetings, when the employee is a member and was invited to participate, or when the sponsoring organization does not require disclosure of a participant employment affiliation, so that the MI participant may collect significant FI made available to general participants.

(2) Specific participation. Specific participation includes:

(a) Collecting significant FI outside the U.S., or from or about non-U.S. persons within the U.S., for CI purposes, at FBI written request.

(b) Collecting significant CI about non-U.S. persons, or U.S. persons who are within DoD investigative jurisdiction. Participation within the U.S. requires FBI coordination.

(c) Identifying and assessing non-U.S. persons as potential FI or CI sources.

(d) Collecting information necessary to identify U.S. persons outside the U.S. as potential sources of assistance for FI or CI.

(e) Developing or maintaining an authorized cover.

d. Undisclosed participation. The following does not constitute undisclosed participation:

(1) Acquisition of goods and services that include incidental issuance of "membership" cards or identification (e.g., video rental cards, library cards, grocery store cards, discount cards, or gymnasium memberships).

(2) Any application, registration or subscription that does not result in actual attendance or participation in the activities of an organization covered under this procedure (e.g., purchase of a subscription to an organization's magazine).

e. Disclosure requirement.

(1) When disclosure is required, the employee's intelligence affiliation will be provided to an executive officer of the organization or to an official in charge of membership, attendance, or the organization records.

(2) Disclosure may be made by the intelligence component element, an authorized NG, Army, AF, or DoD official, or another IC component authorized to make the disclosure on behalf of the NG intelligence component element.

11. **Procedure 11**. Contracting for goods and services.

a. Contracting for goods and services. Procedure 11 of reference d applies to contracting or other arrangements with U.S. persons for the procurement of goods and services by or for an NG intelligence component within the U.S. 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 paragraph 11.d. above apply.

b. Contracts with academic institutions. NG intelligence components 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 components may contract with commercial organizations, private institutions, and individuals within the U.S. 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 (i.e., Internet service provider), and incident to approved activities.

(3) There is a written determination by the Secretary of the Army (ARNG) or Secretary of the AF (ANG) that the sponsorship by an NG intelligence component must be concealed to protect the activities of the intelligence component concerned.

12. **Procedure 12**. Provision of assistance to LE authorities.

a. Requests for NG military support to civilian LE authorities. These requests are closely reviewed and processed separately for approval. 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 IAW Procedure 12 of references d and m. When the requested NG intelligence component capability support to civilian LEAs does not involve FI or CI, it must be processed IAW reference m and must also be approved by the SecDef or his

designee. These provisions apply for NG intelligence support to any federal, state, tribal, or local civilian LEA.

b. Cooperation with LE authorities. Subject to the limitations of paragraph e below, NG intelligence components may cooperate with LE authorities IAW reference m for the purpose of:

(1) Protecting the employees, information, property, and facilities of any element of the DoD or NG.

(2) Investigating or preventing clandestine intelligence activities by foreign powers, international terrorists, or international narcotics operations.

(3) Preventing, detecting, or investigating other violations of law.

(4) Providing specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local LEAs. Provision of assistance by expert personnel shall be approved in each case through NGB-J2 by NGB-JA or applicable general counsel (GC).

(5) Rendering any other assistance and cooperation to LE or other civil authorities not precluded by applicable law.

c. Requesting civilian LEA. Where an NG intelligence component is the lead agency of an investigation, the NG intelligence component may request assistance of a civilian LEA as required.

d. Types of permissible assistance. NG intelligence components may only provide the types of assistance to LE authorities delineated below. Assistance may not be provided for participation in activities that would not be permitted under this instruction.

(1) Violations of U.S. federal law. Incidentally acquired information reasonably believed to indicate a violation of federal law shall be provided to appropriate federal LE officials through J34, AT/FP or LE channels. Disseminate IAW Procedure 4. Protect any applicable sensitive sources and methods.

(2) Other violations of law. Information incidentally acquired during the course of NG CI activities reasonably believed to indicate a violation of state, local, or foreign law will be provided to appropriate officials IAW procedures established by the Army Counterintelligence Coordinating Authority (ACICA) and/or AFOSI. Information incidentally acquired during the course of NG intelligence activities reasonably believed to indicate a violation of state, local, or foreign law will, unless otherwise decided by NGB-J2, Army G2, or AF/A2

for national security reasons, be provided to the appropriate LEA IAW with procedures established by the JFHQ-S J2, or his or her designee. Information covered by this paragraph includes U.S. persons' information, which must be disseminated IAW Procedure 4.

(3) Provision of specialized equipment and facilities. Specialized intelligence equipment and facilities, technical knowledge, or assistance of expert personnel may be provided to federal LE authorities. They also may be provided to state, tribal, and local LE authorities when lives are endangered and only with the approval of the SecDef or his or her designated representative and the concurrence of NGB-J2, IAW reference m.

(4) Assistance of NG intelligence personnel. NG intelligence personnel may be assigned to assist federal LE authorities. They also may be provided to state, tribal, and local LE authorities when lives are endangered only with the approval of the SecDef or his or her designated representative through NGB-J2 IAW reference m.

(5) Assistance to foreign governments or foreign LE. NG intelligence components may render assistance to LEAs and security services of foreign governments or international organizations IAW established policies and applicable SOFAs. The assisting NG intelligence components may not request or participate in activities of such agencies undertaken against U.S. persons that would not be permitted to those components under these procedures.

e. Limitations.

(1) NG intelligence personnel assigned or detailed to Counterdrug (CD) elements supporting civilian LEAs must comply with the rules governing that agency and the rules under which the NG approved their assignment or detail.

(2) NG intelligence elements providing analytical support to civilian LEA will comply with reference n, or the policy of the supported agency. The information under analysis is the property of the supported agency and is not intelligence information. Intelligence elements will provide the raw information and resultant analysis to the civilian LEA, and not retain the data in intelligence files or databases.

(3) NG intelligence component personnel will neither request nor participate in the LE or security activities conducted against U.S. persons by foreign governments or international organizations when the activities would not be authorized in this manual.

f. Procedure 12 Memorandum (P12 Memo). Requests for support requiring approval under this procedure will be through the P12 Memo. The P12 Memo provides details validating the legality of providing NG intelligence component

personnel, specialized equipment, or facilities to LE authorities when they are used to support intelligence functions of those agencies. NG JFHQ-S generates a P12 Memo and seeks approval through NGB-J2 before the execution of a mission. The P12 template is found in Enclosure G. An electronic template is available for download on the NGB-J2 Community of Practice (CoP) located on the J2 Intelink site, reference o.

13. **Procedure 13.** Experimentation on human subjects for intelligence purposes.

a. This procedure applies to the experimentation on human subjects whether or not they are U.S. persons, if conducted by or on behalf of an NG intelligence element. It does not apply to animal experimentation.

b. NG intelligence components do not engage in experimentation involving human subjects for intelligence purposes. Any exception would require approval by the DCS, G-2 (ARNG) or AF/A2 (ANG) and would be undertaken only with the informed consent of the subject and IAW guidelines issued by the Department of Health and Human Services and procedures established by applicable Service regulations and instructions to safeguard the welfare of subjects.

c. Experimentation means any research or testing activity involving human subjects that may expose subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which subjects are ordinarily exposed in their daily lives.

d. Conducted experiments. Experimentation is considered conducted on behalf of an NG intelligence element if:

(1) An NG intelligence element conducts the experiment.

(2) A contractor conducts the experiment on behalf of an NG intelligence element.

(3) A contractor conducts the experiment on behalf of a non-NG intelligence element for NG intelligence benefit.

(4) An NG intelligence element requests the experiment regardless of the existence of a contractual relationship.

14. **Procedure 14.** Employee conduct.

a. Employees of NG intelligence components conduct intelligence activities only IAW references b and d, 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, EO, and applicable regulations and instructions.

b. Employees of NG intelligence components are trained IAW Enclosure B.

c. Employees of NG Intelligence components carry out reporting responsibilities as delineated in Procedure 15.

15. **Procedure 15.** Identifying, investigating, and reporting Questionable Intelligence Activity (QIA), Significant or Highly Sensitive (S/HS) Matters, and Crimes reported to the AG.

a. NG staffs, units, and personnel must report QIA, S/HS matters, and any crimes reported to the AG to the Assistant to the SecDef (ATSD)(IO).

(1) QIA. Any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any EO, or presidential directive is QIA. This includes reference b, this manual, and other regulations, instructions, and policy documents governing that activity, as well as references a, c, and d.

(2) An S/HS matter. A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD intelligence community or otherwise call into question the propriety of an intelligence activity is an S/HS matter. Such matters might be manifested in or by an activity:

(a) Involving congressional inquiries or investigations.

(b) Resulting in adverse media coverage.

(c) Impacting foreign relations or foreign partners.

(d) Related to unauthorized disclosure of classified or protected information, such as information identifying a sensitive source or method. (This does not include reporting routine security violations.)

(3) Crimes reported to the AG are any intelligence activities that have been or will be reported to the AG, or that must be reported to the AG, as required by law or other directive, including crimes reported to the AG, as required by references p.

b. 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 that have no relationship to the intelligence mission (e.g., breach of discipline and simple security or ethics violations) are not subject to IO reporting and will be handled through normal disciplinary and/or LE channels. The NGB-JA or the staff/unit JA can provide assistance in making such determinations.

c. Reporting QIA and S/HS Matters.

(1) NG staffs, units, and personnel must report QIA of a serious nature and all S/HS matters immediately to NGB-IG, NGB-JA, or ATSD (IO) using the supervisory chain of command, where feasible. Such reports may be by any secure means. Oral reports should be documented into a written report as soon as possible afterward.

(2) NG staffs, units, and personnel must report QIA not of a serious nature quarterly to NGB-IG, NGB-JA, or ATSD (IO) using the supervisory chain of command where feasible (e.g., if the supervisor, SIO or commander is involved in the QIA, it is not feasible to use the supervisory chain of command). Such reports are provided to the IG at the first level at which an IG is assigned and not associated with the QIA (e.g., if the unit IG is involved in the QIA, then report to the JFHQ-S IG. If the state IG is also involved, then report to NGB-IG. If the squadron does not have an IG, then report to the wing IG. If the wing does not have an IG, then report to the JFHQ-S IG.) Provide copies to the unit JA and SIO, unless they are involved in the QIA or the IG determines such reporting would be inappropriate. This report must be made regardless of whether or not a criminal or other investigation has been initiated.

(3) A reported allegation does not necessarily mean that a person, staff or unit has violated law or policy. When a QIA report is submitted, it does not reflect negatively upon a unit; rather, it shows staff/unit compliance with this manual. Generally speaking, most QIA occurring during NG domestic operations can easily be remedied through immediate corrective actions.

(4) This Procedure will not be used to satisfy other reporting requirements (e.g., Serious Incident Reports (SIRs) or security violations). Whenever in doubt as to whether an activity should be reported under this Procedure, the activity will be reported as described herein for resolution at the next higher level. Regardless of the reporting channel used, the report must reach NGB-IG no later than five days from discovery.

(5) Description of reports.

(a) Identification of the personnel committing the alleged QIA by rank or civilian grade; security clearance and access; unit of assignment, employment, attachment or detail; and assigned duties at the time of the

activity. Do not identify individuals by name or other personal identifying information unless the NGB-IG so requests.

(b) When and where the activity occurred.

(c) A narrative describing each incident reported.

(d) An explanation of why the incident is being reported either as a potential violation of law, EO, Presidential directive, this manual, other regulation, instruction, or policy. The applicable portion(s) of this manual, references a and d, and/or other applicable EO, law, or policy will be cited.

(e) An explanation of why the incident is considered an S/HS matter, if so reported.

(f) An analysis of how or why the incident occurred.

(g) An assessment of the anticipated impact of the reported incident on national security, international relations, state security, state relations, or NG relations, as well as any mitigation efforts, including success and failures of such efforts. If there has been no impact or no impact is anticipated, the report should so state.

(h) An assessment of any impact the reported incident may have had on civil liberties or protected privacy rights. If there has been no impact or no impact is anticipated, the report should so state.

(i) A description of actions taken if the incident concerns information improperly acquired, handled, used, or destroyed.

(j) Remedial action taken or planned to prevent recurrence of the incident.

(k) Command and/or investigative agency actions planned or ongoing, if applicable. If this report originated outside the affected command, then state when the reporting element notified the affected command. The NGB-IG will then notify the affected command of its responsibility to conduct the inquiry and report updates.

(l) Any additional information that provides context for the incident and is considered relevant for purposes of fully informing the Secretary and/or Deputy SecDef, the Intelligence Oversight Board (IOB), and the Director of National Intelligence (DNI).

(6) Status reports will be submitted to NGB-IG every 30 days until the investigation is complete. When the investigation is complete, submit a final

report to NGB-IG. NGB-JA or the supporting JA must review the final report and include corrective actions planned or implemented, command investigative status, personnel actions, and whether the unit has requested a policy clarification. When an allegation surfaces that is resolved within the five-day time frame specified in paragraph 15.c.(4) above, the report will be submitted as both an initial and a final report.

(7) When an alleged QIA is the focus of a CI or criminal investigation, the investigating agency (e.g., INSCOM, the U.S. Army Criminal Investigation Command (USACIDC), or AFOSI) is responsible to submit an initial notification of QIA to NGB-IG. The investigating agency is not required to provide a 30-day status report to NGB-IG. This manual does not relieve the investigating agency of its normal investigative reporting procedures. When the investigating agency refers its investigative results to the affected command for action, the affected command must submit a final notification to NGB-IG describing the investigative results and corrective actions taken, if any.

(8) When there is doubt about whether an activity should be reported or someone in the chain of command disagrees with a QIA report from a subordinate unit, the lead element will coordinate with the subordinate element to ensure the report meets reportable criteria as listed in paragraphs 16.a. and b above. If the reportable criteria are not met, then the report will be returned with instructions as to the proper reporting channel, if any. If the higher element is in doubt, or the two elements cannot agree, then the report is forwarded to NGB-IG with an analysis of why the report does or does not meet reporting criteria. Before submitting the report, any command may contact the NGB-J2, NGB-IG, or NGB-JA to seek clarification.

(9) Electronic transmittal (i.e., e-mail) is the preferred method for transmission of reports. However, reports may also be transmitted via facsimile (i.e., fax), message, or hard copy, as long as they meet the five-day requirement.

(10) Reports may be classified at any level, including special access program caveats, as necessary, for coherent reporting. If reports have been sent via Secure Internet Protocol Router Network (SIPRNET) or Joint Worldwide Intelligence Communications System (JWICS), then send a notification e-mail on Non-secure Internet Protocol Router Network (NIPRNET).

d. Inquiries.

(1) NG intelligence and intelligence-related staffs and units will inquire into any QIA reported under Procedure 15 (paragraph 16 of this manual), to the extent necessary to determine if the reported activity violates a law, EO, Presidential directive, DoD directive or policy, or an NG regulation, instruction, or policy. Conduct all inquiries as quickly as possible and provide the results

through command channels to NGB-IG. Officials responsible for inquiries may obtain additional assistance from within the component concerned or from other NGB components, as necessary to complete inquiries in a timely manner. The NGB-IG and NGB-JA must have all information necessary to evaluate QIA for compliance with law or policy, regardless of classification or compartmentation.

(2) Each report of QIA must be investigated to the extent necessary to determine the facts and assess if the activity is legal and consistent with applicable policy.

(3) Inquiries into allegations not referred to a CI or criminal investigative agency will be completed within 60 days of the initial report, unless extraordinary circumstances dictate a longer period.

(4) The results will be reported IAW paragraph 16.c above.

(5) Such an inquiry does not alleviate or satisfy the initial five-day reporting requirement in paragraph 15.c.(4) above.

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

(1) Improper collection, retention, or dissemination of U.S. persons information. This includes the following:

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

(b) Producing and disseminating intelligence threat assessments containing U.S. persons information without a clear explanation of the intelligence purpose for which the information was collected (e.g., listing area universities with foreign students or U.S. companies with DoD contracts in an assessment without showing a connection to a foreign power or international terrorism). An exception to this would be an MI element providing direct CI or technology protection support to a DoD contractor.

(c) Incorporating criminal information on a U.S. person into an intelligence product without determining if identifying the person is appropriate.

(d) Collecting U.S. persons information for AT/FP purposes without determining if the intelligence function related to it is authorized (e.g., collecting information on the domestic activities of U.S. persons).

(e) Storing operations and command traffic about U.S. persons in intelligence files merely because the information was transmitted on a classified system.

(f) Collecting open-source U.S. persons information without a logical connection to the unit mission or correlation to a validated collection requirement (e.g., a unit in one area collecting information from the Web page of a militia group in another area, then reporting that information as a CI incident report or disseminating it in unit intelligence products).

(g) Disseminating command AT/FP information on U.S. persons and their domestic activity as an intelligence product (e.g., including U.S. persons groups in an intelligence annex as enemy forces).

(h) Becoming directly involved in criminal investigative activities (e.g., direct participation in a narcotics suspect interrogation) without appropriate mission, authority, and approval.

(i) Identifying a U.S. person by name in an Intelligence Information Report (IIR) without a requirement to do so.

(j) Including the identity of a U.S. person in a contact report when that person is not directly involved with the operation.

(k) Failure to file proper use memorandums (PUM) for domestic imagery collection.

(2) 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.

(3) Misrepresentation. This includes the following:

(a) Using the status of an MI member to gain access for non-MI purposes.

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

(c) Using an MI badge or credentials to represent oneself as an official beyond assigned MI responsibilities; to perform functions not within the mission or authority of the element to which an individual is assigned or attached; or to avoid civil citations, such as off-duty traffic tickets.

(4) QIA constituting a crime. This includes the following:

- (a) Stealing a source payment.
- (b) Using intelligence funds for personal gain.
- (c) Falsifying intelligence or investigative reports.
- (d) Stealing private property while searching for exploitable documents and materiel during a deployment.
- (e) 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.

(5) Misconduct in the performance of intelligence duties. This includes the following:

- (a) Any activity listed in paragraphs 16.e.(1) through (4) above.
- (b) Falsifying investigative reports or personnel security investigation interviews (also known as “curbstoning”).
- (c) Coaching a source or subject of an investigation before an intelligence polygraph examination in an effort to help the individual pass the polygraph.
- (d) Alleged abuse and mistreatment of detainees and prisoners by or directed by intelligence personnel.
- (e) Reports not meeting questionable intelligence activity criteria. The following are examples of reports that do not meet Procedure 15 reporting criteria, unless there is a direct connection to an intelligence activity.
 1. A report of someone acting without authority or exceeding authority that does not describe precisely the nature of the act and which Procedure (1 through 13) or other policy was violated.
 2. Security violations not directly connected to an intelligence activity, such as negligence in handling or storing classified information.
 3. Not following regulations 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.

4. Being absent without leave (AWOL) or having special category absences.

5. Driving while intoxicated (DWI).

6. Drug use or sale.

7. Suicide or attempted suicide.

d. Reporting CI, criminal violations, and federal crimes.

(1) MI personnel. MI personnel also have an obligation to report significant CI activities, criminal cases, instances of espionage, and other possible federal crimes IAW references p and q. This ensures that senior DoD and Department of Justice (DoJ) 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.

(a) Significant CI activities are any CI activities that are significant in and of themselves or that are likely to receive publicity.

(b) Criminal cases. Criminal cases that must be reported are those involving:

1. 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 (GS)/General Grade (GG) grade 15 and above, and the potential loss to the government is \$5,000 or more.

2. Any criminal corruption case related to procurement involving current or retired DoD military or civilian personnel.

3. Any investigation into defective product(s).

(c) 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; 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. It is conduct that is, or may be, a violation of references r and s.

(2) Federal crimes. Reports of federal crimes involving T-32 NG MI personnel will be provided through command channels to NGB-J2 no later than five working days after discovery or receipt. The following will be included in the report:

(a) 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.

(b) When and where the crime occurred.

(c) A description of the federal crime that may have been violated.

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

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

(3) NGB-J2 will transmit reports received under this procedure to NGB-JA, who will review and transmit reports received under this procedure pursuant to procedures adopted by DoJ.

(4) Examples of reportable federal crimes are as follows: espionage, sabotage, unauthorized disclosure of classified information, seditious 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.

(5) Non-reportable federal crimes. The following are examples of non-reportable federal crimes:

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

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

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

(d) Other than homicide or espionage, crimes that were 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 B

NATIONAL GUARD INTELLIGENCE AND COUNTERINTELLIGENCE MISSIONS

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. GEOINT products fall into seven main categories: aeronautical, nautical/hydrographic, topographic/terrestrial, precise positioning and targeting, geodesy and geophysics, geographic names, and GEOINT analysis. IMINT is intelligence derived from the exploitation of collection by visual photography, infrared (IR) sensors, lasers, electro-optical 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. It includes, but is not limited to, full-motion video (FMV), photographic, IR, radar, and electro-optical images captured using ground or aerial-based 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 receiving explicit mission and authority from the SecDef. U.S. persons information 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 D.
3. SIGINT. 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 (CSS) directives and policies, which include references g, h, and i, because they dictate performance boundaries within SIGINT training and operations.
4. HUMINT. HUMINT is a category of intelligence derived from information collected and provided by human sources, both witting and unwitting. HUMINT collection activities include, but are not limited to, conducting source

operations; liaising with host nation (HN) officials and allied counterparts; eliciting information from select sources; debriefing U.S. and allied forces and civilian personnel including refugees, displaced persons (DP), third-country nationals, and local inhabitants; interrogating enemy prisoners of war (EPW) 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. Within the context of the NG, HUMINT activity generally does not involve clandestine activities. NG personnel must have valid mission and authority to conduct any type of HUMINT activity. NG units with a HUMINT mission may conduct training activities with witting participants in a T-32 status during Inactive Duty for Training (IDT) and Annual Training.

5. OSINT. OSINT is intelligence collection from publicly available sources and analyzing it to produce actionable intelligence. In the IC, the term "open" refers to overt, publicly available sources. This includes, but is not limited to, 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 either 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 (e.g., 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 U.S. persons information without proper mission and authority.

7. MEDINT. MEDINT is defined as 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 for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. NG MEDINT personnel will receive IO training IAW Enclosure B. Specific U.S. persons will not be targeted without receiving explicit mission and authority from the SecDef.

8. CI.

a. CI involves gathering information and performing activities to protect against espionage; other intelligence activities; sabotage or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities. NG personnel must have validated mission and authority to conduct any type of surveillance or CI activity.

b. Jurisdiction for domestic CI activities lies with the FBI IAW with reference 1.

c. ACICA exercises technical control, review, coordination, and oversight of Army CI controlled activities. It is the only Army organization that can authorize CI activities within the U.S. and its Territories. The AFOSI provides professional investigative services to commanders of all AF activities. It is the primary organization responsible for AF CI services within the U.S.

d. The NG has no independent authority to engage in real-world CI activity. NG CI agents with badges and credentials can only be involved in CI activities in support of a federal mission or in active service to the U.S. government.

e. ARNG CI units may conduct training activity in a T-32 status during IDT and AT; intelligence products may be produced if training is in support of a national agency or federal mission. Local LEAs must be informed if training activities occur in public areas. Role players/training targets must give prior written consent stating they knowingly are involved in a training exercise.

f. Training relationships with active duty CI organizations is encouraged to enhance training opportunities, but are subject to the same limitations.

g. ANG units/activities are not authorized to engage in independent domestic CI activity or training IAW reference t.

ENCLOSURE C

INTELLIGENCE OVERSIGHT TRAINING REQUIREMENTS

1. Training Requirements.

a. The following personnel must receive IO training:

(1) All NGB, T-32 NG JFHQ-S, and T-32 NG intelligence units and staff organizations, and 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) All T-32 personnel with a core intelligence Military Occupational Specialty (MOS) or Air Force Specialty Code (AFSC) regardless of unit mission, duty title, or assignment.

(4) Contractors or consultants assigned or attached to the units and staffs listed in paragraph (1) above if they are involved in T-32 activities subject to the procedures of DoD 5240.1-R.

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

(6) 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.

(7) All TAGs; commanders, directors, IGs, and JAs or GCs of those organizations who conduct 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/Temporary Duty (TDY) Training. IO monitors 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 development.

(a) All personnel will be familiar with this manual, with emphasis on Procedures 1 through 4, and 12, 14, and 15. The IO monitor will coordinate with his or her servicing IG and JA to provide additional training on IO, or other matters affecting intelligence support keyed to organizational missions and responsibilities.

(b) Training is tailored to the unit mission and will cover, at a minimum, the following:

(1) Scope. The NG IO program pertains to all NG intelligence units and staff organizations, and non-intelligence organizations that perform intelligence or intelligence-related activities. It applies to all military and civilian personnel assigned or attached to these units and staffs on a permanent or temporary basis, regardless of military specialty or job function. It applies to all personnel with core intelligence MOS or AFSC regardless of unit mission, duty title, or assignment. Additionally, it applies to contractors or consultants if they are involved in activities subject to the Procedures of DoD 5240.1-R (reference d and this manual). It applies to NG units and staffs that conduct information operations, which include cyberspace activities, and are components of intelligence organizations. It also applies to all intelligence personnel who support information operations activities with products or services. Furthermore, the program pertains to any person when tasked to perform an intelligence mission regardless of unit of assignment. (See Glossary for the definitions of intelligence and intelligence-related activity.)

(2) Permissible activities. NG intelligence units and staffs can collect, process, retain, and disseminate intelligence on U.S. persons only if it is necessary to the conduct as a function or mission assigned to the component involved, and only if it falls within one of the 15 categories listed under reference d and in Procedure 2. In the U.S., it is not generally within the mission of military intelligence units to collect information on U.S. persons; this would, however, normally be within the mission of CI units. Although some information on U.S. persons may be “publicly available” (one of the 15 categories referred to above), this does not obviate the unit mission/function requirement. NG intelligence units and staffs must be familiar with Procedures 1, 2, 3, and 4, which provide general information and guidance on collection, retention, and dissemination of U.S. persons information; Procedure 14, which stipulates the professional responsibilities of personnel to carry out intelligence

or intelligence-related activities IAW any governing policy or regulation pertaining to the activity in this procedure or any other governing policy or regulation; and Procedure 15, which defines reporting responsibilities.

(3) Collection techniques. The method of collection must be the least intrusive means possible to accomplish the mission/function. Procedures 5 through 11 govern the more intrusive forms of collection. These special collection activities include the following: electronic and communications surveillance (Procedure 5), concealed monitoring (Procedure 6), physical searches (Procedure 7), examination of U.S. mail (Procedure 8), physical surveillance (Procedure 9), undisclosed participation in an organization (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. NG intelligence components must be familiar with any procedures concerning collection techniques used by their unit. Include a discussion of intelligence component-specific policy that implements these special collection activities and how intelligence component operations and collection will be carried out in compliance with this instruction and the implementing policy.

(4) Law Enforcement assistance. There are also very specific procedures and restrictions on providing intelligence support to LEAs. NG intelligence units and staffs providing assistance to LEAs must be familiar with Procedure 12, which provides this guidance.

(5) QIA. IO is much broader than just collecting, retaining, and disseminating intelligence on a U.S. person. All NG intelligence component personnel are required to report QIA, defined "as any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any executive order or Presidential directive, including reference b, or applicable DoD policy, including reference d. Procedure 15 defines this requirement to report and investigate misconduct incident to intelligence and intelligence-related activities that violate the laws, policies, or regulations governing those activities.

(6) Reporting. NG staffs, units, and personnel must report QIA to NGB-IG, NGB-JA, or ATSD (IO) using the supervisory chain of command. Such reports will be expeditiously provided to the IG at the first level at which an IG is assigned and not associated with the QIA, with copies to the JA and, unless the IG determines such reporting would be inappropriate, to the SIO at the same level. This report must be made regardless of whether a criminal or other investigation has been initiated. A reported allegation does not necessarily mean that a person, staff, or unit has violated law or policy. The fact that a QIA report has been submitted does not reflect negatively upon a unit; rather, it shows a staff/unit's compliance with this instruction. Whenever in doubt as to whether an activity should be reported, the activity will be reported for

resolution at the higher level. Regardless of the reporting channel used, the report must reach NGB-IG no later than five days from discovery. NG intelligence component personnel must be familiar with local policy and procedures for reporting QIA.

(7) The Internet. While much of the information posted on the Internet is publicly available, an intelligence professional acting in an official capacity still must have the official mission 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 also applies to information found on SIPRNET, JWICS, and other classified media.

(8) Reminder. Even though most intelligence personnel are not "collectors," most do retain and disseminate intelligence. Some personnel, such as those working with domestic imagery collection or information warfare programs, may need a more in-depth understanding of select aspects of intelligence oversight rules and procedures. These topics must be included in IO training if conducted by the intelligence component.

(c) To develop tailored training, units may download data from the IO folders in the Guard Knowledge Online (GKO), Army Knowledge Online (AKO), or AKO-SIPRNET IC collaboration portals; the AF Distributed Learning System (ADLS) and AF portal; the ATSD (IO) website; or other appropriate Web pages. All are encouraged to periodically check the NGB IO folder on the Joint Intelligence Directorates Current Intelligence Division CoP on the GKO portal (NIPRNET: <https://www.intelink.gov/sites/ngb-j2/J23n/default.aspx>) as well as the website maintained by the ATSD (IO) (NIPRNET: www.dod.mil/atsdio; SIPRNET: www.atsdio.ismc.sgov.gov/atsdio/; or JWICS: www.atsdio.ismc.ic.gov/atsdio/) for soft copies of the basic intelligence oversight references, additional training aids/software, a list of frequently asked questions/intelligence oversight examples, and other useful information. Other techniques that can be used to raise awareness are poster campaigns/visual aids and messages posted in newsletters or on bulletin boards.

3. Training records. Organizations will maintain records of personnel 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.

4. Additional training requirements for SIGINT units. Commands with SIGINT crypto logic elements will ensure that those elements obtain appropriate training from qualified personnel on applicable SIGINT directives. Reference g delineates policies and procedures to ensure that the missions and functions of the U.S. SIGINT System (USSS) are conducted in a manner that safeguard the

constitutional rights of U.S. persons. All USSS personnel who collect, process, retain, or disseminate SIGINT information must read and be familiar with its contents. All NG commands that have SIGINT cryptologic elements must also be aware of NSA reporting requirements for SIGINT, as routine continental U.S. (CONUS) garrison-based IO reporting responsibilities vary greatly from reporting requirements while in T-10 status.

ENCLOSURE D

DOMESTIC OPERATIONS

1. Homeland Defense (HD).

a. HD is 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.

b. Certain NG units have been assigned roles in support of HD missions, including Air Defense of the Homeland and Anti-Missile Defense of the Homeland missions. 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 d.

2. Homeland Security.

a. The Homeland Security mission consists of intelligence activities that are related to homeland security threats and is conducted by a subcategory of National Security Intelligence, the Department of Homeland Security (DHS) Intelligence Enterprise. NG intelligence components with the mission and authority may collect, analyze, and disseminate information IAW Procedures 2 through 4 of this manual and reference d.

b. The link between Homeland Security Intelligence and the NG is so strong, that in many states, TAG is also the State Director of Homeland Security. 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 are the following: Is there a foreign connection? Is it part of the element's mission essential task list (METL)? Is it within the purpose of the funding being used? Are the activities overt and transparent? And finally, has any U.S. persons' information been properly safeguarded and have their rights to privacy been protected?

3. Defense Support of Civilian Authorities (DSCA) intelligence activities.

a. General Information. NG intelligence components may provide support to local, tribal, state, and federal civilian authorities, which includes support to LE, civil disturbance support, restoration of order, and support requests for National Special Security Events (NSSEs) (e.g., political conventions and major

sporting events), actual or potential disasters or catastrophic incidents (including pandemics, hurricanes, floods, earthquakes, terrorist attacks, or large-scale industrial accidents), or other emergencies, when requested by a primary agency and approved by the SecDef or a designee, or as directed by the President.

b. SAR. At the request of local, tribal, state, or the AF Rescue Coordination Center (AFRCC), NG intelligence units may provide support for SAR missions. U.S. persons' information may be collected during SAR missions; if a person is at risk of death or injury, consent is implied. However, once the SAR mission is over, all U.S. persons information will be purged. During exigent circumstances (i.e., when life and limb are at stake), states may seek verbal authorization to collect domestic imagery. However, all approvals must be followed in writing with a PUM as soon as practicable thereafter.

c. IAA.

(1) NG intelligence component personnel and equipment may be used for IAA to fulfill TAG requirements for situational awareness or planning purposes, or upon receipt of an NG JFHQ-S or NGB-validated primary agency/lead federal agency Request for Assistance (RFA). IAA activities will not be used to collect U.S. persons information. 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 (MA) from the Federal Emergency Management Agency (FEMA).

(2) When authorized by the SecDef, NG intelligence capabilities may provide support to federal, state, local, and tribal agencies in certain IAA mission sets, including situational awareness, SAR, damage assessment, evacuation monitoring, CBRNE assessment, hydrographic survey, and dynamic ground coordination IAW reference u.

(3) Capabilities. NG intelligence component capabilities authorized for non-intelligence activities include the following:

(a) Analysis of imagery, geospatial data, and information collected from cameras, video, electro-optical, IR, and Forward-Looking Infrared Radar (FLIR), and the dissemination of final products based on that analysis.

(b) Analysis of information collected from government agencies operating within their lawful functions and authorities.

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

(4) Imagery. Including optical, electro-optical, FMV, and IR, imagery collected during DSCA operations may be shared with other DoD entities (to include NGB) and civil authorities, and state authorities as required based on validated need.

(a) Civil authorities are authorized to disclose (i.e., show) or release selected Unclassified imagery products for official use only (FOUO) to participating or affected private citizens when the disclosure/release would prevent injury or loss of life, or facilitate disaster mitigation and recovery efforts.

(b) Specific imagery products may be released to the U.S. media during senior official press conferences to provide visual depiction of disaster area status and disaster response activities.

(c) Imagery released to private citizens and U.S. media will not include imagery depicting DoD installations or other sensitive areas.

4. NG Baseline Operating Posture.

a. The NG operates on a day-to-day basis in the NG Baseline Operating Posture and conducts required planning, training, and exercises, as well as ongoing mandated domestic operations in this posture. The general focus of the NG Baseline Operating Posture is to maintain NG readiness to conduct all assigned missions in both its state and federal roles. Additionally, the NG maintains situational awareness of the Homeland operational environment and conducts mandated ongoing operations. Extensive training, deliberate planning, and preparation are required, as well as mission-specific planning and training.

b. Authorized NG intelligence activities in the NG Baseline Operating Posture include assisting in deterring and preventing attacks on the Homeland; maintaining well-trained and well-equipped units prepared to conduct or support state or federal missions; maintaining situational awareness and detecting threats or concerns by conducting any mandated ongoing domestic operations (e.g., CD support).

(1) JIPOE.

(a) Every NG operation, even within the 50 states, the District of Columbia, and the Territories and possessions of the U.S., regardless of size, must have access to intelligence. When operating within the U.S., NG intelligence components must gear their intelligence assets toward understanding the environment and providing information that will be necessary for senior decision makers at key decision and decisive points, all

the while protecting the Constitutional, privacy, and civil rights of U.S. persons by adhering to the procedures, guidelines and principles in this manual.

(b) If the NG is lawfully participating in a DSCA mission, information on non-DoD affiliated persons and organizations may be acquired if it is essential to meet operational requirements. However, there must be a link between the U.S. persons information to be collected and the NG intelligence component's assigned mission and function. There are limits on the use of NG intelligence component capabilities to support civilian LEA. Any requests for intelligence support to LEAs must be separately staffed and approved before mission execution. NG intelligence components may not task, direct, or request missions in direct support of LE, unless authorized IAW Procedure 12 of this manual and reference d, and reference m by the SecDef.

(2) CD support.

(a) NG CD programs support the LEA linguist and criminal intelligence analysis activities. Criminal information comes into temporary possession of NG members supporting LEAs, but is not retained by the NG. CD coordinators will coordinate with LEAs to ensure intelligence support of LEA operations is conducted IAW this manual, reference d and other applicable directives, and in the support role intended by CD Support Program policy. IO training, with an emphasis on the handling, protection, distribution, and destruction of U.S. persons information, will be included in doctrinal training given to each member at initial entry and repeated annually for all personnel (See reference v for additional information.).

(b) Supported LEAs are responsible for obtaining legal authorization required to permit information gathering and must document agreements in support of the LEA IAW reference v.

(3) Civil Support Teams (CSTs) and other non-intelligence units.

(a) NG CSTs, CBRNE Response Force Package (CERFP), and Homeland Response Force (HRF), collectively known as the CBRNE Enterprise, advises and facilitates in areas that have been or may be attacked with suspected Weapons of Mass Destruction (WMD) agents, advises civilian responders on appropriate actions through on-site testing and expert consultation, and facilitates the arrival of additional state and federal military forces. These units will comply with provisions outlined in reference n concerning the handling of information related to non-DoD-affiliated persons. Intelligence personnel assigned 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 d.

(b) While conducting operations, CBRNE Enterprise units could incidentally or otherwise collect U.S. persons information. Upon completion of operations, all information or files must be redacted of all U.S. persons information before being used in After Action Reports (AARs), Mission Termination Packets, or other follow-up reports.

(4) Critical Infrastructure Protection-Mission Assurance Assessment (CIP-MAA) Detachments. The CIP-MAA Detachments conduct all-hazard risk assessments on prioritized federal and state critical infrastructure in support of the Defense Critical Infrastructure Program (DCIP). 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 d.

ENCLOSURE E

DOMESTIC IMAGERY

1. General.

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

b. Domestic imagery for the purposes of this manual is defined as any newly collected or archived imagery collected by satellite (national, tactical, or commercial) or airborne platforms for intelligence or intelligence-related purposes that cover the land areas of the 50 states, the District of Columbia, and the U.S. Territories and possessions, to a 12 nautical mile (NM) seaward limit of these land areas. This section provides policy and guidance regarding domestic imagery collected by NG intelligence components. This does not apply to non-intelligence units using non-intelligence platforms (e.g., Civil Air Patrol (CAP)) to obtain domestic imagery for non-intelligence purposes.

c. Domestic imagery. The following generally constitute legally valid requirements for domestic imagery:

(1) Responses to natural disasters and civilian emergencies. 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, and other natural disasters.

(2) CI, FI, and Security-related vulnerability assessments. This category of information supports operations security (OPSEC) during intelligence and security activities involving federal property or private property where consent has been obtained as appropriate.

(3) Requirements in support of environmental studies of wildlife, geologic features, or 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 in support of system or satellite calibration, algorithm, or analytical developments and training or weapon systems development or training.

(5) Requirements for imagery in support of LE activities when authorized under Procedure 12 of this manual and reference d, including imagery in support of counternarcotics operations and NSSEs. Follow the IO rules detailed in Execute Orders (EXORDs) for LE support.

d. 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.

2. Domestic imagery from national satellites. The National Geospatial-Intelligence Agency (NGA) is responsible for the policy and legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites. NG components must follow policy and procedures established in reference w reference x. NG intelligence components must submit requirements for new collection to NGA through NGB-J2 (T-32) or through gaining combatant command (COCOM) or major command (MACOM (Army) or MAJCOM (AF)) (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.

3. Domestic imagery from airborne platforms. The Defense Intelligence Agency (DIA) is responsible for the policy and legal review and approval of requests to collect and disseminate domestic imagery from airborne platforms. An approved PUM must be on file with NGB-J2 (T-32) or the gaining COCOM, MACOM, or MAJCOM (T-10) before airborne platforms can be tasked to collect domestic imagery under any of the following conditions.

a. The use of intelligence, surveillance, and reconnaissance (ISR) or IAA platforms, assets, or personnel to collect sensor data; the use of intelligence analysts, systems, or organizations to analyze sensor data; or the use of sensor data for intelligence, intelligence-related, or IAA purposes.

b. The PUM must be IAW this manual and applicable DIA policy and guidance (references y and z), applicable EOs, and DoD regulations. During an emergency or crisis where U.S. Northern Command (USNORTHCOM) is designated as lead DoD Operational Authority, all related requests for domestic imagery from airborne platforms must be coordinated with USNORTHCOM to ensure compliance with proper use provisions IAW reference s aa and bb.

4. Domestic imagery from commercial satellites. NG intelligence components may obtain NGA domestic commercial satellite imagery (e.g., Web-based Access and Retrieval Portal-Unclassified National Information Library (WARP-UNIL) and the Saint Louis Information Library (STIL) and successor systems) 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 components may also use domestic open-source or publicly available imagery (e.g., U.S. Geological Survey (USGS) imagery, Google Earth imagery, and Falcon View Imagery). However, an internal memorandum for record (MFR) describing the purpose of the domestic imagery and naming the component official approving the use will be retained on file in all cases. If obtained imagery specifically identifies a U.S. person (e.g., private property), then follow the rules contained in Procedures 2-4 for collection, retention, and dissemination in this manual and reference d. Pay particular attention to procedures regarding retention. NG intelligence components must not appear to be collecting, exploiting, or disseminating commercial imagery or imagery-associated products for purposes other than the approved mission. Reference cc contains additional information on commercial imagery use.

5. Fighter, Bomber, Remotely Piloted Aircraft (RPA), Unmanned Aircraft System (UAS), and Unmanned Aerial Vehicle (UAV) navigational/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 for the purpose of gathering 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 RPA, UAS, and operations, exercise, and training missions will not conduct nonconsensual surveillance on any specifically identified U.S. persons, unless expressly approved by SecDef, IAW U.S. law and regulations. Civil LEAs, such as the U.S. Customs and Border Protection (CBP), FBI, U.S. Immigration and Customs Enforcement (ICE), and the U.S. Coast Guard, will handle all such data.

c. Tracking will only be conducted on approved vehicles in which the owner/operator has given consent to the unit to conduct the tracking.

d. NG UAS, UAV, and RPA assets will NOT be employed for DSCA purposes without specific SecDef approval IAW reference dd.

6. PUM and Proper Use MFR.

a. PUM.

(1) A PUM is a memorandum that defines a request by an organization for a domestic imagery requirement and its intended use. A PUM acknowledges awareness of the legal and policy restrictions regarding domestic imagery collection, retention, dissemination, and use. PUMs can be classified or unclassified depending on content. The PUM is written on the organization letterhead and signed by the organization certifying official, a field grade officer 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 the rights of U.S. citizens and organizations are being protected IAW the law. Failure to file a PUM before the conduct of a domestic imagery collection mission is QIA, reportable to the ATSD (IO).

(2) Any NG JFHQ-S that owns or has operational control over NG assets that conduct domestic imagery activities within the U.S., Territories, and District of Columbia is responsible for creating and seeking approval for a PUM before the execution of a domestic imagery collection mission. In a T-32 status, the JFHQ-S J2 will route PUMs to NGB-J2 as outlined in paragraph 5 on page E-6. NGB-J2 will forward the PUM to NGB-JA and NGB-IG for review. Once the document is found to be sufficient, NGB-J2 will approve the PUM and notify the requesting state. In a T-10 status, route PUMs to the gaining COCOM, MACOM or MAJCOM J2, A2, or G2, who will forward the PUM to the appropriate IG and JA for oversight and legal review.

(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 (e.g., IAA missions in support of the Kentucky Derby, IAA missions in support to hurricane response efforts, and training missions in support of the National Level Exercise (NLE)).

(4) PUMs will include the following:

(a) Subject line. Identify the document as a PUM for a domestic imagery request. If the PUM is directed to NGA for approval, then the subject line will identify the document as a PUM and include a tracking number (e.g., PUM NGB-11-001).

(b) Paragraph 1. State in non-technical terms the purpose of the request, intended use of the imagery, time frame for collection of new imagery or for intended use of archived imagery, and the supported mission, training, operation, and project or exercise name. If the requested imagery is of a military property, then also state the following:

1. The imagery is requested for a military or related national security purpose.
2. The request is not made on behalf of, and will not be provided to, any federal, state, or local LEAs.
3. The requested imagery and any classified, imagery-derived products created will be made available only to authorized personnel for the purpose stated.
4. The target or focus of the imagery is current U.S. military property either owned or leased by the federal government.
5. The proposed collection will not target non-U.S. military activities or facilities, U.S. persons, or private properties, and such collection will only occur if the imaging of the target property is under control of a U.S. military organization.
6. Non-military activities on the targeted U.S. military property will not be exploited.

(c) Paragraph 2. Identify the named area of interest or target of collection, including, if applicable:

1. Type of named area of interest or target, state/territory/possession, geo-coordinates, and Basic Encyclopedia (BE) number. If the diameter of a target is over 10 NM, then provide corner vertices and the Directed Search Area (DSA)/Line of Communication (LOC) number.
2. For archived imagery, include satellite or airborne mission name and date, pass and frame/ops number.

(d) Paragraph 3. Specify the organizations that are to receive the imagery (or derived products, briefings, publications), the desired format, and where the imagery will be stored.

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 format of the imagery (e.g., digital, tape, paper print, duplicate positive, negative, etc.), quantity, and any special production requirements.

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

(e) Paragraph 4. Provide one of the following "proper use" statements:

1. Airborne imagery. "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. Satellite imagery.

a. "Approved recipients of this domestic imagery must meet the following criteria if they intend to store the domestic imagery approved by this PUM on an information system. First, the domestic imagery may only be stored on information systems of approved recipients. Second, the approved recipients who store domestic imagery must ensure that it is properly monitored for the approved period and that it is removed when the approved period expires. Third, the cognizant security office must certify that the domestic imagery is being stored on an information system that is certified and accredited under reference ee and that access to the domestic imagery is restricted to only approved recipients. Any request to further disseminate imagery products produced under this PUM will require an amendment or separate proper use approval."

b. "I certify that the intended collection and use of the requested information, materials, and imagery derived from classified and unclassified overhead systems are in support of congressionally approved programs of *[insert requesting organization's name]* and do not violate applicable laws, including the statutory authority of *[Insert the requesting organization's name]*. The request for imagery is not for the purpose of targeting any specific U.S. persons 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."

(f) Paragraph 5. The following "I am authorized" paragraph: "I am authorized as a trusted agent and certifying official on behalf of *[Insert the requesting unit's name]*, and I understand that I am responsible for the accuracy of the information contained herein and for the proper safeguarding of products received in response."

(g) Paragraph 6. Name and contact information of J2 certifying official (must be a field grade officer or civilian equivalent).

(h) Paragraph 7. Certification that State JA and IG have reviewed the PUM and found it sufficient; date of this review; and name and contact information of State JA and IG.

(i) Paragraph 8. Name, office, telephone number, and e-mail address or fax number for PUM point of contact.

(j) Signature authority. The signature of the certifying official (must be a field grade officer or civilian equivalent).

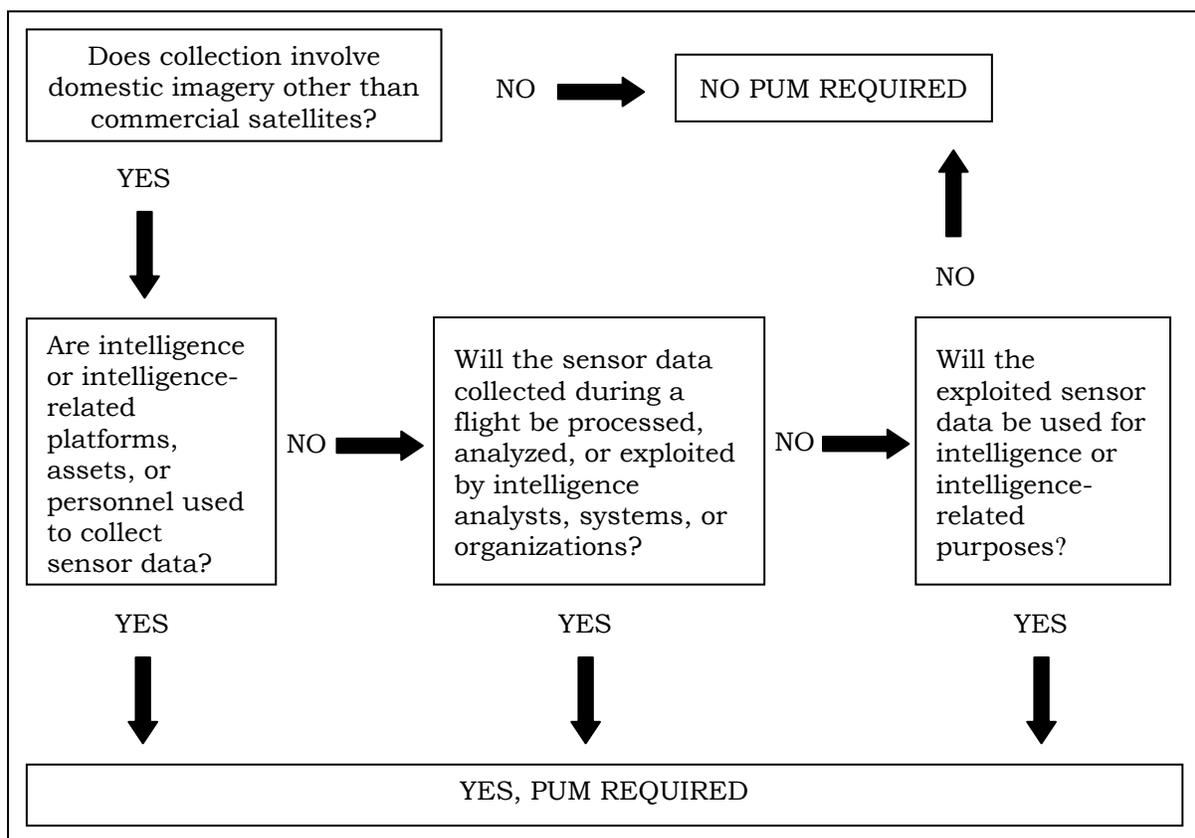


Figure 2. Is a PUM Required?

(5) A generic PUM template and sample may be found in Enclosures L and M. This generic PUM template and a specific PUM template for Geospatial Information Interoperability Exploitation – Portable (GIIEP) are available electronically for download, see reference ff. It is unacceptable to have a long-term PUM sitting on the shelf for each and every DSCA event. Each PUM that supports an emerging DSCA disaster, operation, or training effort will need to be tailored to each individual event and legally approved each time.

(6) Staffing procedures for airborne platform PUMs.

(a) T 32.

1. Approval resides with NGB-J2.

2. Requests will be submitted to NGB-J2 via fax at 703-601-2263 or e-mail to NGGBJ2IO@ngb.army.mil.

3. NGB-J2 will coordinate the PUM review and approval with NGB-IG and NGB-JA.

(7) NGB-J2. NGB-J2 will provide timely responses back to the requesting staff/unit that will include an official memorandum of approval and any additional procedural requirements, if necessary.

(a) T 10.

1. Approval resides with the gaining COCOM J2 or MACOM/MAJCOM G2/A2.

2. Requests will be submitted to the combatant J2 or MACOM/MAJCOM G2/A2 IAW its established policy and procedures.

3. The COCOM J2 or MACOM/MAJCOM G2/A2 will coordinate PUM approval IAW its established policy and procedures.

b. Proper Use Memorandum for Record (Proper Use MFR). The Proper Use MFR describes the purpose of the collection, retention, and/or dissemination of commercial satellite domestic imagery. It is signed by the intelligence organization's certifying official, who is also, in effect, approving the use of the imagery. The Proper Use MFR should be retained on file one year after expiration. It may be re-certified if the imagery is still required.

7. 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 to include the lawful acquisition of U.S. persons information when that support is consistent with the Constitution and other laws, regulations, and instructions. The NG JFHQ-S must implement the proper safeguards to protect all information and products collected, acquired, received, or used during emergency response and ensure all applicable security regulations and guidelines, and other restrictions are followed. In such cases, a report will be made immediately to the CNGB through the NG Coordination Center (NGCC). A PUM will be filed with NGB-J2 as soon as possible thereafter.

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 Enclosure I for a sample amended PUM. Domestic imagery used in briefings, reports, or publications may not be used for any purpose other than that for which it was originally requested. The use of domestic imagery in briefings, reports, or publications may require additional review if the audience goes beyond the scope of the approved PUM. Under reference u, domestic imagery previously collected under the SecDef's authority and used for DoD intelligence component capabilities for missions other than intelligence activities that support DSCA missions, such as for IAA, may not be retained for future DSCA pre-event planning or for FI or CI purposes without additional review and authorization. If the authority was requested through command channels to the SecDef at the time of the original missions, and that use is also addressed in the PUM, then the data may be used. Conversely, domestic imagery previously collected for FI or CI purposes may not be used for DSCA support missions without proper authority and review for proper use.

b. Once a military organization receives authorized domestic imagery of military property, the imagery may be used in briefings, reports, analytical products, and other publications as long as the military organization ensures that the proposed use is IAW the purpose for which that imagery was originally collected or requested. For example, a training publication containing domestic imagery of military property distributed within a limited military training or exercise environment would be appropriate. Distribution of the publication throughout the military or the IC without prior approval would be inappropriate.

c. A PUM must be submitted for publications that contain text and domestic imagery obtained from classified national reconnaissance platforms.

d. Unless otherwise approved, domestic imagery must be withheld from all general access database systems (e.g., Intelink). Controlled or limited access share folders or drives, password protected websites, password protected portals, and e-mail distributions to authorized individuals 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 (e.g. Intelink or SIPRNET) cannot access domestic imagery without an appropriate authorization or control measure. Access must be limited to those with a need to know.

9. Analysis 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 (i.e., 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. A PUM is not required for access to the NGA commercial satellite imagery archives for federal-related purposes. The onus of compliance IAW reference d is on the requestor and the agency accessing the data. For example, NASA, a non-intelligence organization, is not subject to IO policy or reference d; therefore, they have full access to the commercial archives for scientific research. All use of the imagery must comply with the enhanced view license.

c. A requesting organization must clearly communicate within its PUM who the exploitation entities are, if 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 target.

10. Special applications of domestic imagery.

a. Imagery collected during FI and CI activities authorized under Procedure 9 (Physical Surveillance). Domestic imagery may be collected from ground and airborne platforms provided that collection against the specific target has been approved IAW Procedure 9.

b. Generally, classified domestic imagery may not be used in direct support of domestic LE activities. An organization may not attempt to support federal, state, or local LE with classified domestic imagery without prior approval.

c. Domestic disaster assessment conducted on behalf of federal civilian agencies.

(1) Requesting classified domestic imagery to support manmade or natural disasters is carried out at the request of federal civilian agencies by the IC pursuant to the Economy Act (reference gg) or the Robert T. Stafford Disaster Relief and Emergency Assistance Act (reference hh). Using the established PUM procedures and their inherent efficiencies for domestic collection eliminates the need for submission and coordination for each event. However, any unforeseen exceptions can be addressed via telephone or other expedient means with the PUM amendments to follow as soon as possible.

(2) Under reference hh, FEMA, representing the needs of Federal Response Framework participants, may request classified domestic imagery collection after coordinating with the Interagency Remote Sensing Coordination Cell (IRSCC). Other federal civil agencies having missions for specific disaster response or environmental research for disaster prevention also may request classified domestic imagery through the authority of the IRSCC.

(3) When requested by the primary agency, the military organizations function as part of the National Response Framework and, therefore, coordinate their collection needs with the primary agency. The military may also request classified domestic imagery collection when military facilities are endangered or for baseline analysis. When federal civil agencies are involved, the overall domestic collection strategy will come under the authority of the federal civil agency with the appropriate disaster mission.

(4) Other than safeguarding its own facilities and installations, the DoD intelligence component has no domestic disaster mission, but may provide appropriate support under the Economy Act, Stafford Act, or other applicable statutory authority when asked to participate by federal civil agencies. Under these circumstances, use of DoD intelligence component capabilities for other than intelligence activities may be approved by the SecDef through NGB-J2.

d. Public Affairs use of domestic imagery.

(1) Media and public interest in IAA and intelligence-related DSCA activities can be intense and immediate. Participants in any IAA or intelligence-related DSCA activity will coordinate with the unit or organization public affairs officer (PAO). Personnel should refer all media inquires and other requests for information from outside of NG/LEA channels to the PAO. The supported LEA should take the lead concerning Public Affairs and make the final determination concerning release of information to the public in coordination with the PAO. In the CD mission, the PAO should consult with CD coordinators to determine whether news releases pose OPSEC issues.

(2) 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 to ensure no sensitive military or government facilities are visible. 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 U.S. Once imagery is released to the public, the NG and DoD no longer have any control over its use or onward dissemination. Therefore, DIA mandates that all imagery be reviewed and its

CNGBM 2000.01
26 November 2012

contents verified to confirm the need for release and to confirm the right level of information is released to proper organizations IAW the PUM.

ENCLOSURE F

PROPER USE MEMORANDUM FORMAT

Print on State Letterhead

[Insert date]

MEMORANDUM FOR NGB-J2

SUBJECT: *[Insert state Military Department, Joint Force Headquarters - State, or National Guard] Airborne Imagery Proper Use Memorandum (PUM) for [Insert the exercise, operation, or mission and its date(s)]*

1. (U//FOUO) References:

- a. (U) EO 12333, United States Intelligence Activities, 4 Dec 81, as amended.
- b. (U) Chairman, Joint Chiefs of Staff (CJCS) Message, DTG 191905Z Aug 11, subject: Standing DSCA EXORD.
- c. (U) DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, Dec 82.
- d. (U) DIA Message, DIA/CL DTG 282048Z Nov 01, subject: New Procedures for the Approval of DoD Domestic Airborne Reconnaissance Imagery Proper Use Statements.
- e. (U) DIA Message, DIA/CL, DTG 231845Z Sep 96, subject: Proper Use Statements for Domestic Imagery – Updated Guidance (S).
- f. (U) CNGBI 2000.01, National Guard Intelligence Activities, XX September 2012
- g. (U) Insert local IO guidance.

2. (U//FOUO) This PUM covers *[Insert affected areas (e.g. missions to be flown over Northern Nevada and California, including Washoe, Carson, Storey, Lyon, Douglas, and Churchill counties in Nevada and Sierra, Nevada, Placer, El Dorado Amador, and Alpine counties in California)]*. *[Insert the mission purpose (e.g. These missions are to assess the insert types of damage caused by insert catastrophic event)]*. *[Insert airborne platforms and sensors (e.g. Airborne platforms to be used include the C-130 Scathe View, Predator UAS and Raven UAS. Airborne sensors to be used include Full-Motion Video (EO and IR) and Synthetic Aperture RADAR)]*. All platforms, sensor data, and imagery products will be used in a support role of local, state, and federal officials *(modify as necessary)* during these missions. *[IF RPA/UAS/UAV assets are included, then insert “National Guard UAS assets will NOT be employed for DSCA operations, including support to Federal, State, local, and tribal government organizations, without specific SecDef approval IAW DoDI 3025.18.”] [Indicate whether SIGINT, HUMINT, or MASINT will be collected or disseminated. If so, then address*

collection platforms and sensors to be used and the specific mission(s) for which they'll be used.

3. (U//FOUO) No U.S. persons will be targeted during these operations. Any personally identifying information unintentionally and incidentally collected about specific U.S. persons will be purged and destroyed unless it may be lawfully retained and disseminated to other governmental agencies that have a need for it IAW DoD 5240.1-R, CNGBI 2000.01, and other applicable laws, regulations, and policies.

4. (U//FOUO) Sensor data and imagery resulting from these collection efforts will be processed and exploited by *[Insert relevant systems, personnel, and organizations]*. Raw imagery, analytic data, working copies, and finished products will be used by *[Insert key personnel, organizations, and purpose (e.g. local and state first responders, CA National Guard, NGB, NORTHCOM, Florida Military Department, and Incident Command Centers for the purpose of damage assessments, Defense Support to Civil Authorities (DSCA) operations, and future support planning)]*. *[Insert formats to be used (e.g. Products will be disseminated in hard copy and be available online via a secure server at insert IP address)]*. *[Insert retention and disposal procedures to be used.] [Insert IO training received by the personnel who will be handling these products.]*

5. (U//FOUO) I certify that the intended collection and use of the requested information, materials, and imagery are in support of Congressionally approved programs and are not in violation of applicable laws. The request for imagery is not for the purpose of targeting any specific U.S. person, 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.

6. (U//FOUO) CERTIFICATION: I am authorized as trusted agent and certifying official on behalf of the requesting unit, and I understand I am responsible for the accuracy of the information contained herein and for the proper safeguarding of products received in response. *[Insert the point of contact (POC) and contact information of the individual certifying accuracy of the collection, retention, and dissemination of the imagery -- must be a field grade officer or civilian equivalent.]*

7. (U) This proper use statement for domestic imagery was reviewed and approved by the *[Insert the name of the state office responsible for IO compliance - insert the specific individual's title and name]* for compliance with law, policy, and intelligence oversight on *[Insert the date]*.

8. (U) Point of contact for this PUM is *[Insert the POC's name and contact information]*.

[Insert Signature]
[Insert Signature Block
(must be field grade officer or
civilian equivalent,
(e.g., J2, Intelligence Officer (S2), A2,
SIO, unit commander)]

ENCLOSURE G

AMENDED PROPER USE MEMORANDUM FORMAT

Print on State Letterhead

[Insert date]

MEMORANDUM FOR NGB-J2

SUBJECT: Amendment to *[Insert the name of the original PUM, dated DD MMM YY]* (U)

1. (U) References:

- a. EO 12333, *United States Intelligence Activities*, 4 Dec 81, as amended.
- b. CJCS Standing DSCA EXORD (U), DTG 191905Z AUG 11.
- c. DoD Regulation 5240.1-R, Dec 82 (U) *Activities of DoD Intelligence Components that Affect United States Persons*.
- d. DIA Message, *New Procedures for the Approval of DoD Domestic Airborne Reconnaissance Imagery Proper Use Statements*, DTG 282305ZNov01.
- e. DIA/CL Message, (S) *Proper Use Statements for Domestic Imagery – Updated Guidance*, DTG 231845ZSep96.
- f. CNGBI 2000.01, *National Guard Intelligence Activities*, 17 September 2012.
- g. *[Insert local IO guidance]*.

2. (U/FOUO) This amendment to subject PUM *[Insert any changes to mission purpose, collection, retention, exploitation, analysis, and/or dissemination]*.

Sample 1: This amendment to subject PUM extends effective date from DD MMM YY to DD MMM YY.

Sample 2: This amendment to subject PUM adds the following additional areas affected by Hurricane Irene: XXX.]

3. (U) POC for this PUM is *[Insert the POC's name and contact information]*.

[Insert Signature]
[Insert Signature Block
(must be field grade officer or civilian
equivalent)
(e.g., J2, S2, A2, SIO, unit commander)]

ENCLOSURE H

PRIVATE CORPORATATION LETTER OF CONSENT FORMAT

1. Not all situations require letters of consent. Examples of situations that may require a letter of consent are as follows: 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.

2. 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.

[Print on Company Letterhead]
[Insert date]

The *[Insert the state 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 state 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]

ENCLOSURE I

PRIVATE INDIVIDUAL LETTER OF CONSENT FORMAT

1. Not all situations require letters of consent. Examples of situations that may require a letter of consent are as follows: 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.
2. 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.

[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 (e.g., my levee, my 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]

ENCLOSURE J

PROCEDURE 12 MEMORANDUM FORMAT

Print on State letterhead

[Insert Date]

MEMORANDUM FOR SecDef
THRU NGB-J2

SUBJECT: Support to LE under Procedure 12, DoD Regulation 5240.1R for the *[Insert the name of LEA]* (U)

1. (U) References:
 - a. EO 12333, 4 Dec 81, United States Intelligence Activities.
 - b. DoD Regulation 5240.1-R, Dec 82 (U) Activities of DoD Intelligence Components that Affect United States Persons.
 - c. DoD Regulation 5525.5, Cooperation with Civilian Law Enforcement Officials.

2. (U//FOUO) Memorandum for record on authorization for *[Insert the state military organization]* to provide support to LE Under Procedure 12, DoD Regulation 5240.1R to *[Insert the name of the LEA]*. The *[Insert the name of the LEA]* requested the use of National Guard intelligence components to support *[Insert a specific description of support requested to include the number of personnel and/or quantity/type of equipment]*. This mission is essential to the *[Insert justification]* and does not adversely affect the readiness of the intelligence component. All *[Insert a description of products to be developed, if any]* will be used in a direct support role of *[Insert the name of the LEA]* officials. No other forms of domestic collection are covered by this request.

3. (U//FOUO) Types of Missions in support of *[Insert the name of the LEA]*: Cooperation with the *[Insert the name of the LEA]* is consistent with limitations contained in references b and c, and Procedure 12. B. 1. c. for the purposes of preventing, detecting, or investigating violations of the law.
 - (1) (U) *[Insert a description of the support]* to aid in *[Insert the mission/purpose]*.

 - (2) (U) National Guard personnel and/or equipment will be under *[Insert the name of the LEA]* authority and control.

 - (3) (U) National Guard personnel are *[Insert location(s)]*.

(4) (U) National Guard personnel will support the mission from *[Insert date, not to exceed 60 days]*.

4. (U//FOUO) Information will be processed and exploited only on *[Insert the name of the LEA]* information systems. Raw analytic data, working copies, and finished products will be the responsibility of *[Insert the name of the LEA]* and will not be retained by the National Guard.

5. (U//FOUO) Personnel have been trained in IO and the request for support is consistent with the constitutional and other legal rights of U.S. persons. I am authorized as a trusted agent and certifying official on behalf of the intelligence component and I understand I am responsible for the accuracy of the information contained herein and for the proper safeguarding of products received in response.

6. (U//FOUO) I have consulted with General Counsel *[Insert his or her rank and name]* and Inspector General *[Insert his or her rank and name]* and they concur with the use of the *[Insert state]* National Guard intelligence component for the purposes stated above.

7. (U) The POC is the undersigned at *[Insert phone number]*.

*[J2/ SIO sign-block
(must be field grade officer)]*

ENCLOSURE K

INTELLIGENCE SUPPORT TO FORCE PROTECTION

1. General.

a. 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 components 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.

b. As a general rule, FP operations within the U.S. are the primary responsibility of civilian federal, state, and local LE authorities. In the U.S., NG intelligence components will limit FP collection to FI and international terrorism threat data. The NGB and NG JFHQ-S Provost Marshall (PM) or J34 provide NG leadership with information and recommendations to support decision-making pertaining to AT/FP, critical infrastructure, security, and LE activities. This activity requires review, analysis, and distribution of significant and relevant LE information. NGB, NG JFHQ-S PM, and J34 may receive and disseminate time-sensitive threat information within the U.S., regardless of source or type. As non-intelligence entities, they are not subject to the provisions of this regulation, but must comply with reference n.

c. However, when foreign groups or persons threaten DoD personnel, resources, or activities, NG intelligence components may intentionally target, collect, retain, and disseminate this information.

d. NG intelligence personnel may receive information from LEAs, other organizations, or sources that contain U.S. persons' information. Merely receiving information does not constitute collection. Information is considered collected only when it has been received for use by an employee of a DoD intelligence component in the course of his or her official duties.

e. 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 AT/FP mission. Security, FP or LE, not intelligence personnel, should lead the meeting. The chart in Figure 3 illustrates how information should flow between J2 and PM/J34, and how the two elements share and handle sensitive information IAW both IO policy and reference n.

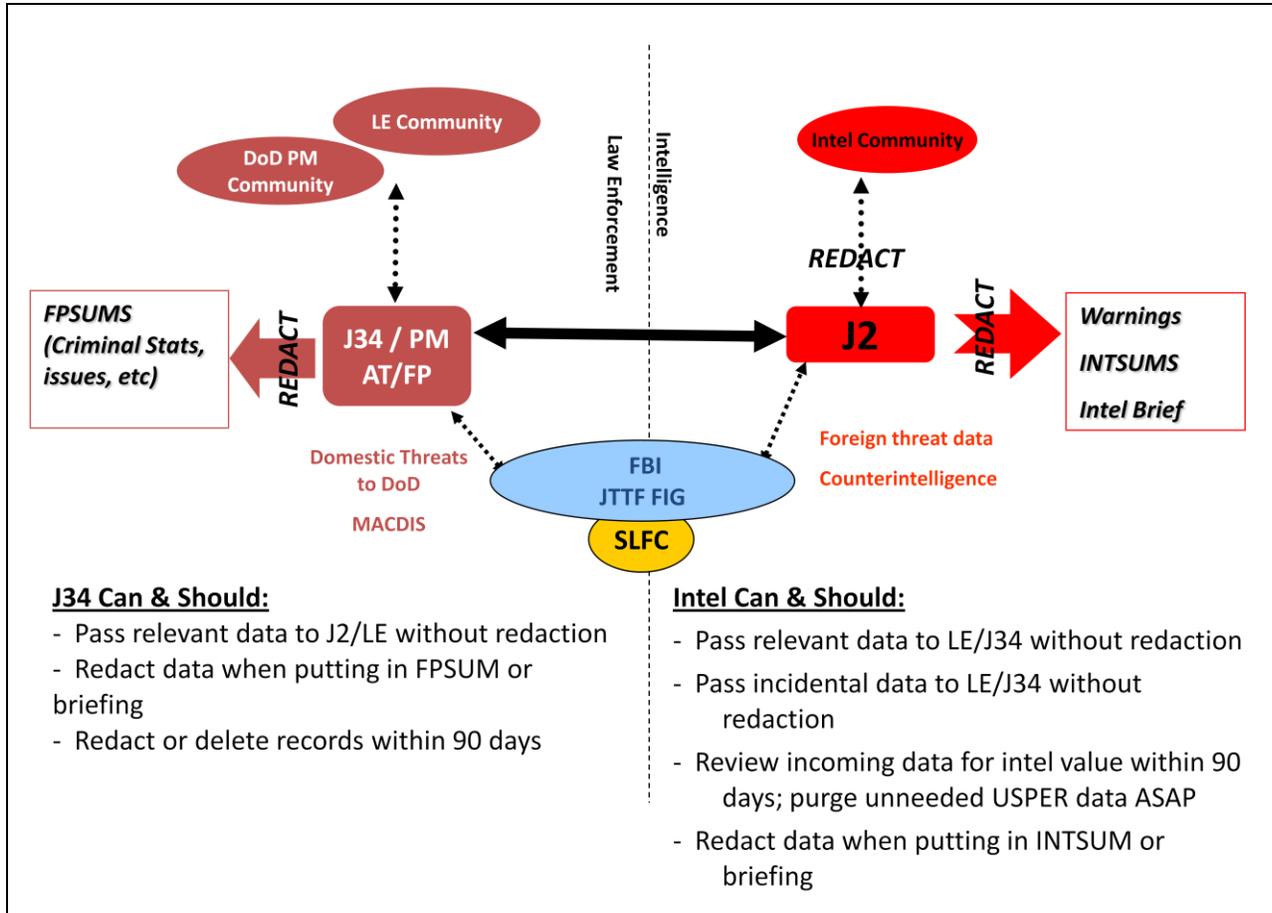


Figure 3. Sensitive Information Handling

f. Consolidated (MI and criminal intelligence data) threat assessments cannot be filed, stored, or maintained as an intelligence product. These assessments must be filed, stored, and maintained within operational channels. NG intelligence component elements will not control FP databases within the U.S. NG intelligence components that are assigned an FP mission may only collect US persons' information IAW the procedures in this manual and reference d. Coordinate with the appropriate LE unit/agency before collecting information on any U.S. individual or domestic group for FP purposes.

g. 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 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.

h. NG intelligence assets with the mission to support FP, may assist in fusing LE, CI, and intelligence information in support of FP (e.g., AT and/or LE activities), consistent with IO procedures. Criminal intelligence containing U.S. persons' information 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 intelligence if there is no specific U.S. persons information or if the U.S. persons information is redacted, even if no direct threat to the NG exists, but the LEA or IC agency has included the information in threat summaries or intelligence products because that non-specific information is necessary to conduct a NG mission. For instance, a state fusion center intelligence product may include information on a new improvised explosive device (IED) technique used by a U.S. white supremacy group. The NG JFHQ-S J2 may then refer to the new method of making the explosive, but redact the U.S. persons information.

i. With approval from the SecDef, 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, electro-optical, IR, and FLIR 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, AT/FP, and/or PM Personnel. When personnel are not available, it is permissible to dual-hat intelligence and AT/FP or PM personnel, but this practice is highly discouraged given the propensity for IO violations and the risk of potential QIA. Consolidated databases and files are not permitted. A clear separation between intelligence, AT/FP, and PM channels must be maintained.

3. Reporting Incidentally Acquired Threat Information.

a. If during the course of routine activities and authorized missions, NG intelligence components receive information, which includes U.S. persons information, on potential threats to life, limb or property, then the information must be passed to appropriate authorities. Receipt of U.S. persons information does not constitute a QIA or other IO violation. Intelligence personnel will route and ensure such information 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 immediately notifies the appropriate entities with authority to counter threat (e.g., Post/Base Command

Section, Military Police/Security Forces/PM, FBI, Municipal Police Department, etc.).

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

d. Threat information may only be withheld from dissemination upon the approval of ARNG-G2 or AF/A2 for FI or ACICA (Army) or Commander, AFOSI (AF) for CI, and only for national security reasons.

ENCLOSURE L

MULTI-NATIONAL AND STATE PARTNERSHIP PROGRAM INTELLIGENCE
ACTIVITIES

1. Within multinational commands and state partnership programs (SPPs), NG intelligence component personnel are still subject to the provisions of reference b and d, and this manual. If a foreign nation allows its personnel to conduct activities that U.S. personnel are not permitted to do, then a non-U.S. multi-national intelligence unit commander may direct or authorize unit personnel to do so; however, U.S. personnel may not participate. Conversely, a U.S. military commander of a multi-national unit or SPP may not direct non-U.S. personnel to conduct activities that are lawful under other nations' laws, but prohibited by reference b and c, EO12333, DoD 5240.1-R, and this manual. The NGB-JA must review NG multi-national or SPP intelligence activities for U.S. legal sufficiency.
2. All NG intelligence component personnel will adhere to DoD and Service security, debriefing, and foreign disclosure policy when conducting foreign travel.

ENCLOSURE M

COMPUTER NETWORKS

1. General.

a. NG intelligence components are increasingly conducting intelligence and CI activities on the Internet. While much of the information posted on the Internet is publicly available, NG intelligence components 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 also applies to information found on SIPRNET, JWICS, 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. IP Addresses.

a. An IP address is a numeric string (e.g., 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. 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 Web. Sometimes, the information available is very general and does not allow one to determine if the IP address constitutes information about a U.S. person. In other instances, the information that is available 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."

b. However, 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 or not 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. Nevertheless, some Internet service providers (ISPs) principally provide service to a U.S.-based clientele. An IP address within a block assigned to such an ISP 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 (e.g., 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.

a. An e-mail address 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. 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 (e.g., smitgj@ or smi2345@). Others plainly identify an individual (e.g., 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, though, 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.

b. 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 U.S. that any e-mail account with that provider should be presumed to be associated with a U.S. person (e.g., George.Smith@ng.army.mil). This latter category of e-mail addresses may only be collected, retained, or disseminated IAW the requirements of IAW references ii and d. All other e-mail addresses may be treated in a manner 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 components 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. For e-mail addresses that are cryptic, it may be near 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 Locators (URL).

a. 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 (e.g., George_Smith.com or USSTEEL.com). In other instances, the words in a URL do not convey, in any apparent way, information concerning persons (e.g., Bicyclists.com). 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 (e.g., .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. (e.g., .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 or not 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 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.

b. Unlike IP and e-mail addresses, URLs are almost by definition, publicly available. As such, even if they identify U.S. persons, lists of URL addresses may be maintained by NG intelligence components provided such collection is within the scope of an authorized intelligence/CI activity assigned to that component. NG intelligence components also may open the websites associated with such URLs if doing so is part of an authorized mission. If, however, the component wants to collect information beyond what is available on the website, then it must make an effort to determine whether the person about whom they are collecting is a U.S. person and, if so, comply with IO procedures.

ENCLOSURE N
THE IO CONTINUITY BINDER

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

1. Appointment letters for Primary and Alternate IO Monitors
2. IO Monitor duties and responsibilities
3. Unit IO Training
4. IO training records (initial, annual, and pre-deployment)
5. Copies of the following IO Reference Documents:
 - a. EO 12333 (reference b)
 - b. DoDD 5240.01 (reference c)
 - c. DoD 5240.1-R (reference d)
 - e. DoDD 5148.11 (reference jj)
 - f. CNGBI 2000.01 (reference a)
 - g. CNGBM 2000.01 (this manual)
 - h. Army Regulation (AR) 381-10 (Joint Staffs and ARNG Units) (reference e)
 - i. AFI 14-104 (Joint Staffs and ANG Units) (reference f)
 - j. State IO standard operating procedure (SOP) or policy
6. Unit-oriented IO Checklist
7. Self-inspection and inspection records
8. QIA process and report format
9. Copies of any QIA reports
10. Annual file review certification MFR

ENCLOSURE O

COMPLIANCE INSPECTION GUIDANCE

1. Normally, NGB, ARNG, and ATSD (IO) inspectors do not use checklists during their IO inspections. Generally speaking, the inspectors will request mission briefings from all intelligence and intelligence-related units and staffs, and discuss their 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 unauthorized U.S. persons information has been retained, and may interview personnel to ensure they are aware of basic IO requirements (e.g., what constitutes a U.S. person, what constitutes a QIA, what obligation do personnel have to report QIA, to whom should personnel report QIA, that no retaliatory action can be taken for reporting QIA, and where to find applicable IO directives, regulations, and policies). All will provide a verbal outbrief upon completion of the inspection. Inspectors from NGB and ARNG will follow up with a written report.
2. The NGB IG team will use reference oo for inspections of NG T-32 IO programs.
3. An ATSD (IO) Inspection Guide is available on the ATSD(IO)websites. See references kk, ll, and mm.
4. According to attachment 3 of reference f, AF inspectors, staff assistance visit (SAV) team members, and units will follow its guidance to assess compliance by intelligence units and staffs with the rules and procedures pertaining to collecting, retaining, and disseminating intelligence on U.S. persons and the adequacy of the IO programs.
5. All units and staffs subject to IO will perform a self-inspection in the final quarter of the calendar year if the organization has not been evaluated in the current calendar year by IGs from at least one of the following organizations: ATSD (IO), MACOM, MAJCOM, ARNG, ANG, or NGB. Maintain a copy of self-inspection results in the IO Policy or Continuity Book.

ENCLOSURE P

THE INTELLIGENCE OVERSIGHT PROCESS

1. U.S. persons information may be 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 15 authorized categories.

2. Special collection techniques require additional approval. The flow chart depicted in Figure 4 represents the decision making process when considering how to handle U.S. persons information in the course of conducting NG intelligence and intelligence-related missions and functions.

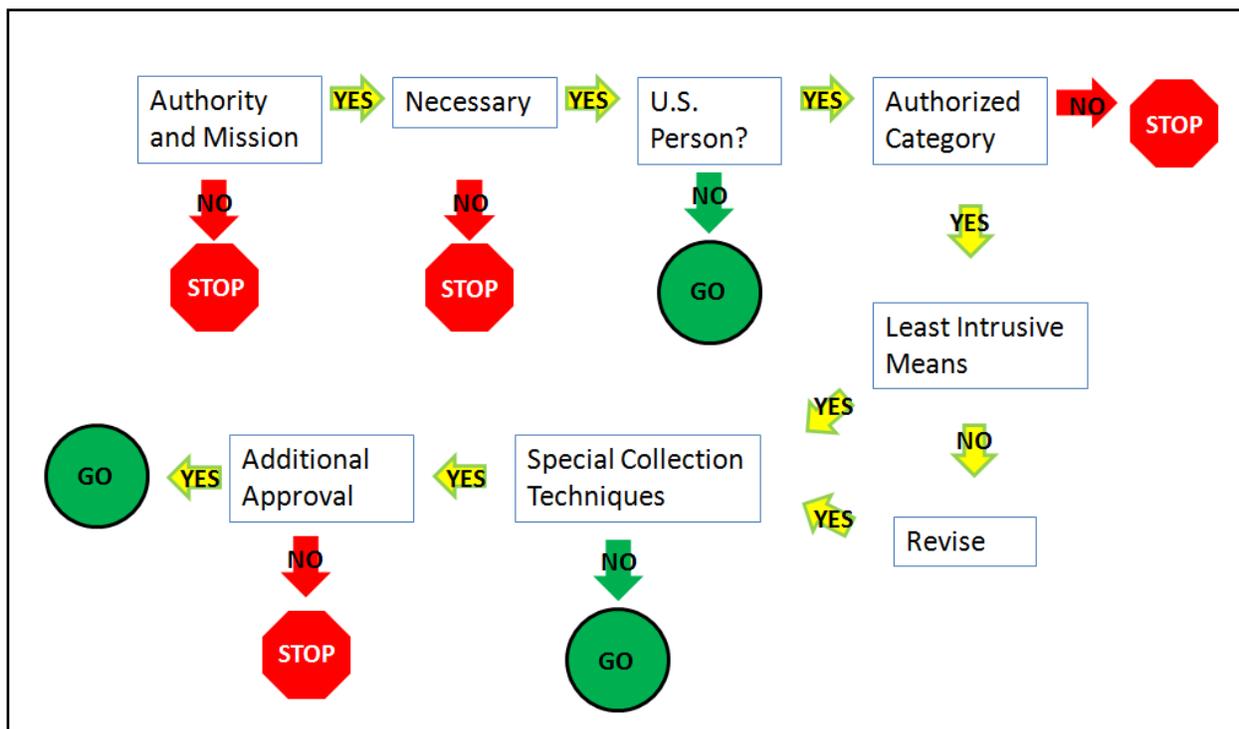


Figure 4. The Intelligence Oversight Process

Step 1. Do you have the authority and mission to collect, process, analyze, retain, and/or disseminate the intelligence? If not, then stop; do not collect, process, analyze, retain and/or disseminate the intelligence. Your defined mission may be found in EXORDs, operation orders (OPORDs), an EMAC, USSIDs, FEMA MAs, and/or SecDef memorandums.

Step 2. You have the authority and mission, but is collecting, processing, analysis, retention, and/or dissemination of the intelligence necessary to

successfully carry out your defined mission/function/task? If not, then stop; do not collect, process, analyze, retain, and/or disseminate the intelligence.

Step 3. Is U.S. persons information involved? If not, then collect, process, analyze, retain, and/or disseminate the intelligence. If U.S. persons' information is involved, then continue to Step 4.

Step 4. Does the information to be collected, processed, analyzed, retained, and/or disseminated fall within one of the 15 authorized categories? If not, then stop; do not collect, process, analyze, retain, and/or disseminate the intelligence. If yes, then continue to Step 5.

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.

Step 6. Does the collection involve any special collection techniques? Special collection activities include the following: electronic and communications surveillance (Procedure 5), concealed monitoring (Procedure 6), physical searches (Procedure 7), examination of U.S. mail (Procedure 8), physical surveillance (Procedure 9), undisclosed participation in an organization (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.

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

ENCLOSURE Q

SAMPLE INTELLIGENCE OVERSIGHT WALLET CARD

 UNCLASSIFIED	Intelligence Oversight Card Ref: EO 12333, DoD 5240.1-R, AFI 14-104, AR 381-10
<p>Military Intelligence personnel SHALL NOT collect (e.g., concealed monitoring, mail/physical searches, electronic/physical surveillance or undisclosed participation), retain, or disseminate information about a U.S. person unless done IAW the procedures contained in DoD Regulation 5240.1-R and only if the information falls into one or more of the following categories:</p>	
<ul style="list-style-type: none">- Information Obtained with Consent- Publicly Available Information- Foreign Intelligence- Counterintelligence- Potential Sources of Intelligence- Protection of Intel Sources/Methods- Physical Security- Personnel Security- Communication Security- Narcotics- Threats to safety- Overhead Reconnaissance- Administrative Purposes	
UNCLASSIFIED	

<p>U.S. Person: A U.S. citizen; a known permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; or, a corporation, if incorporated in the U.S. and not directly controlled by a foreign government. Any person or organization located outside the U.S. is presumed NOT to be a U.S. persc UNLESS there is specific information to the contrary.</p> <p>Any conduct that constitutes or is related to an intelligence activity th: may violate the law must be reported. Employees are encouraged to submit such reports through command channels but may report directly to the IG and JA. (DoD 5240.1-R)</p> <p>PRIMARY IO MONITOR:</p> <p>ALTERNATE MONITOR:</p> <p>INSPECTOR GENERAL:</p> <p>JUDGE ADVOCATE:</p>
--

ENCLOSURE R

REFERENCES

- a. CNGB Instruction 2000.01, 17 September 2012, "National Guard Intelligence Activities"
- b. Executive Order 12333, December 4, 1981, "United States Intelligence Activities," (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))
- c. DoD Directive 5240.01, 27 August 2007, "DoD Intelligence Activities"
- d. DoD 5240.1-R, December 1982, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons"
- e. Army Regulation 381-10, 3 May 2007, "U.S. Army Intelligence Activities"
- f. Air Force Instruction 14-104, 23 April 2012, "Oversight of Intelligence Activities, 23 April 2012"
- g. U.S. Signals Intelligence Directives (USSID) SP0018 (S), 27 July 2003
- h. USSID, SE10000 (Army) (U)
- i. USSID, 1600NG (ARNG)(S) and 3500 (ANG)(S)
- j. Department of Justice (DoJ)-DoD Memorandum of Understanding Reporting of Information Concerning Federal Crimes, dated August 1999
- k. DoD 4525.6-M, 15 Aug 2002, "Department of Defense Postal Manual"
- l. The Undersecretary of Defense, Policy Memorandum, 16 April 1979, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigations" (C)
- m. DoD Directive 5525.5, 15 Jan 1986, "DoD Cooperation with Civilian Law Enforcement Officials"
- n. DoD Directive 5200.27, 7 Jan 1980, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"
- o. J2 Intelink website: <<https://www.intelink.gov/sites/ngb-j2>>

- p. Memorandum of Understanding Between the Attorney General and the Secretary of Defense, "Reporting of Information Concerning Federal Crimes," August 1995
- q. DoD Instruction 5240.04, 2 Feb 2009, "Reporting of Counterintelligence and Criminal Violations"
- r. 18 United States Code (U.S.C.) § 371, "Conspiracy to commit offense or to defraud United States"
- s. 50 U.S.C. § 783, "Offenses"
- t. Air Force Instruction (AFI) 71-101, Volume 4, 1 August 2000, "Counterintelligence"
- u. Chairman, Joint Chiefs of Staff (CJCS) Standing Defense Support to Civil Authorities (DSCA) Execution Order (EXORD), DTG 102000Z Sep 10
- v. NGR 500-2/ANG Instruction 10-801, 31 March 2000, "National Guard Counterdrug Support"
- w. The National Security Act of 1947, 50 United States Code § 401, et sequentia, as amended
- x. NGA National System for Geospatial-Intelligence Manual (NSGM) FA 1806, May 2011, "Domestic Imagery"
- y. DIA Message, *Proper Use Statements for Domestic Imagery – Updated Guidance (U)*, DTG 231845Z Dec 96
- z. DIA Message, *New Procedures for Approval of DoD Domestic Airborne Reconnaissance Imagery Proper Use Statements*, DTG 282350Z Nov 01
- aa. North American Aerospace Defense Command (NORAD) and USNORTHCOM Instruction 14-3, 5 May 2009, "Domestic Imagery"
- bb. USNORTHCOM Instruction 14-103, 16 April 2007, "*Intelligence Oversight*"
- cc. National Geospatial-Intelligence Agency Commercial Imagery Guide, 2011
- dd. DoDD 3025.18, December 29, 2010, "Defense Support of Civil Authorities (DSCA)"

- ee. Intelligence Community Directive (ICD) Number 503, 15 Sept 2008, “Intelligence Community Information Technology System Security Risk Management, Certification and Accreditation”
- ff. <<https://www.intelink.gov/inteldocs/browse.php?fFolderId=59635>>
- gg. Public Law 100-707, June 2007, “Robert G. Stafford Disaster Relief and Emergency Assistance Act”, as amended
- hh. The Economy Act, March 20, 1933, as amended
- ii. DoD Office of General Council Memorandum, 06 February 2001 “*Principles Governing the Collection of Internet Addresses by DoD Intelligence and Counterintelligence Components*”
- jj. DoD Directive 5148.11, 21 May 2004, “Assistant to the Secretary of Defense for Intelligence Oversight (ATSD (IO))”
- kk. <NIPRNET: <http://atsdio.defense.gov/welcome.html>>
- ll. <SIPRNET: www.atsdio.ismic.sgov.gov/atsdio/>
- mm. <JWICS: www.atsdio.ismic.ic.gov/atsdio/>
- nn. DoD Instruction 5505.7, January 27, 2012, “Titling and Indexing Subjects of Criminal Investigations in the Department of Defense”
- oo. National Guard Regulation (NGR) 20-10/Air National Guard Instruction 14-1-1, 13 June 2011, “National Guard Inspector General Intelligence Oversight Procedures”

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS.

A2	Director of Intelligence (Air Force)
AAR	After Action Report
ACICA	Army Counterintelligence Coordinating Authority
ADLS	Air Force Distributed Learning System
AF	Air Force
AFI	Air Force Instruction
AFOSI	Air Force Office of Special Investigations
AFRCC	Air Force Rescue Coordination Center
AFSC	Air Force Specialty Code
AG	Attorney General
AKO	Army Knowledge Online
ANG	Air National Guard
AR	Army Regulation
ARNG	Army National Guard
AT/FP	Anti-Terrorism/ Force Protection
ATSD (IO)	Assistant to the Secretary of Defense for Intelligence Oversight
AWOL	Absent Without Leave
BE	Basic Encyclopedia
CAP	Civil Air Patrol
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CD	Counterdrug
CERFP	CBRNE Response Force Package
CI	Counterintelligence
CIA	Central Intelligence Agency
CIP-MAA	Critical Infrastructure Protection-Mission Assurance Assessment
CJCS	Chairman, Joint Chiefs of Staff
CNGB	Chief National Guard Bureau
CNGBI	Chief National Guard Bureau Instruction
COCOM	Combatant Command
COMSEC	Communications Security
CONUS	Continental United States
CoP	Community of Practice
CSS	Central Security Service
CST	Civil Support Team
DCIP	Defense Critical Infrastructure Program
DCS	Deputy Chief of Staff
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency

DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
DP	Displaced Persons
DSA	Directed Search Area
DSCA	Defense Support to Civil Authorities
DWI	Driving While Intoxicated
EMAC	Emergency Management Assistance Compact
EO	Executive Order
EPW	Enemy Prisoner of War
EXORD	Execute Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FI	Foreign Intelligence
FLIR	Forward-Looking Infrared Radar
FMV	Full-Motion Video
FOUO	For Official Use Only
FP	Force Protection
G2	Director of Intelligence (Army)
GC	General Counsel
GEOINT	Geospatial Intelligence
GG	General Grade
GIIEP	Geospatial Information Interoperability Exploitation – Portable
GKO	Guard Knowledge Online
GPS	Global Positioning System
GS	General Schedule
HD	Homeland Defense
HN	Host Nation
HRF	Homeland Response Force
HUMINT	Human Intelligence
IAA	Incident Awareness and Assessment
IAW	In accordance with
IC	Intelligence Community
ICD	Intelligence Community Directive
ICE	Immigration and Customs Enforcement
IDT	Inactive Duty for Training
IED	Improvised Explosive Device
IG	Inspector General
IIR	Intelligence Information Report
IMINT	Imagery Intelligence
INSCOM	United States Army Intelligence and Security Command
IO	Intelligence Oversight
IOB	Intelligence Oversight Board
IP	Internet Protocol
IR	Infrared

IRSCC	Interagency Remote Sensing Coordination Cell
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
J2	Joint Director of Intelligence
JA	Judge Advocate
JFHQ-S	Joint Force Headquarters-State
JIPOE	Joint Intelligence Preparation of the Operational Environment
JWICS	Joint Worldwide Intelligence Communications System
LE	Law Enforcement
LEA	Law Enforcement Agency
LOC	Line of Communication
MA	Mission Assignment
MACOM	Major Command (Army)
MAJCOM	Major Command (Air Force)
MASINT	Measurements and Signatures Intelligence
MEDINT	Medical Intelligence
METL	Mission Essential Task List
MFR	Memorandum for Record
MI	Military Intelligence
MOS	Military Occupational Specialty
NG	National Guard
NG JFHQ-S	National Guard Joint Force Headquarters-State
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NGCC	National Guard Coordination Center
NIPRNET	Non-secure Internet Protocol Router Network
NLE	National Level Exercise
NM	Nautical Mile
NORAD	North American Aerospace Defense Command
NSA	National Security Agency
NSGM	National System for Geospatial-Intelligence Manual
NSSE	National Special Security Event
OPORD	Operation Order
OPSEC	Operations Security
OSINT	Open-source Intelligence
P12 Memo	Procedure 12 Memorandum
PAO	Public Affairs Officer
PM	Provost Marshall
POC	Point of Contact
PUM	Proper Use Memorandum
QIA	Questionable Intelligence Activity
RFA	Request for Assistance
RPA	Remotely Piloted Aircraft
S2	Intelligence Officer (Army)
SAD	State Active Duty

SAR	Search and Rescue
SAV	Staff Assistance Visit
SecDef	Secretary of Defense
S/HS	Significant or Highly Sensitive
SIGINT	Signals Intelligence
SIO	Senior Intelligence Officer
SIPRNET	Secret Internet Protocol Router Network
SIR	Serious Incident Report
SOFA	Status of Forces Agreement
SOP	Standard Operating Procedure
SPP	State Partnership Program
STIL	Saint Louis Information Library
T-10	Title 10
T-32	Title 32
TAG	The Adjutant General
TDY	Temporary Duty
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
URL	Uniform Resource Locator
U.S.	United States
USACIDC	United States Army Criminal Investigation Command
USD(I)	Undersecretary of Defense for Intelligence
USPS	United States Postal Service
USGS	United States Geological Survey
USNORTHCOM	United States Northern Command
USSID	United States Signals Intelligence Directive
USSS	United States SIGINT System
WARP-UNIL	Web-based Access and Retrieval Portal-Unclassified National Information Library
WMD	Weapons of Mass Destruction
WWW	World-Wide Web

PART II. DEFINITIONS.

Air National Guard -- That part of the organized militia of the several 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 sixteenth clause of section 8, article I of the Constitution; is organized, armed, and equipped wholly or partly at Federal expense; and is federally recognized IAW reference dd

Army National Guard -- That part of the organized militia of the several 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 sixteenth 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 IAW this instruction and other applicable policy.

Chief, National Guard Bureau (CNGB) -- The head of the National Guard Bureau (NGB), which is a joint activity of the Department of Defense (DoD), and is the highest ranking officer in the National Guard (NG) and the NG of the United States; the latter of which is a joint reserve component of the U.S. Army and U.S. Air Force. The CNGB serves as the principal advisor to the Secretary of Defense (SecDef), through the Chairman of the Joint Chiefs of Staff (CJCS), on matters involving non-federalized NG forces and on other matters as determined by the SecDef. The CNGB also serves as the principal adviser to the Secretary of the Army, Secretary of the Air Force (AF), the Chief of Staff of the Army, and the Chief of Staff of the AF, on matters relating to federalized forces of the NG of the U.S. and its subcomponents; the Army National Guard (ARNG) and Air National Guard (ANG) of the U.S.

Collection -- Information is considered collected only when it has been received in the course of official duties by an employee of a National Guard (NG) intelligence component and is permanently retained for intelligence purposes, or is temporarily retained for the purpose of evaluating whether it may be permanently retained for intelligence use. Information identifying a U.S. person is permanently retained whenever an employee of an NG intelligence component takes an action that demonstrates intent to use such information, such as producing an intelligence information or incident report or adding the information to an intelligence database. Data acquired by electronic means (e.g., signals traffic analysis, telemetry, or measurement and signals intelligence) is collected only when it has been processed from digital form into a form intelligible to a human. Information downloaded or copied from the Internet and placed into an intelligence database or other data storing medium is deemed to have been collected.

Counterintelligence (CI) -- Information gathered and activities conducted to 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 activities, but not including personnel, physical, document, or communication security programs.

Criminal Intelligence -- Information gathered or collated, analyzed, recorded/reported, and disseminated by LEA concerning types of crime, identified criminals, and known or suspected criminal groups.

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 (DoD) components -- The Office of the Secretary of Defense (SecDef), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands (COCOMs), the Office of the Inspector General (IG) of the DoD, the Defense Agencies, the DoD field activities, and all other organizational entities within DoD.

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 U.S., to a 12 nautical mile seaward limit of these land areas. National Guard (NG) units may, at times, require newly collected or archived domestic imagery.

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 (PUM) and is not a reflection of a change in the organization mission. Generally reflects ad hoc requirements for domestic imagery.

Department of Defense (DoD) Intelligence Components -- All DoD organizations that perform national intelligence, Defense intelligence, and intelligence-related functions, including: the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve components of the Military Departments, including the U.S. Coast Guard when operating as a service in the Navy.

Eagle Vision -- The Eagle Vision system is a deployable ground station for processing imagery received directly from commercial satellite platforms.

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, which includes Federal departments, agencies, establishments, corporations (e.g.,

Tennessee Valley Authority), boards, committees, commissions, councils, and quasi-official agencies (e.g., Smithsonian Institution).

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.

Foreign Connection -- Reasonable evidence of ties to foreign powers, individuals, or organizations. This includes international terrorist or narcotic activities through direct communications with other members, membership, or training in a terrorist organization and declaring allegiance to and adoption of terrorist ideology. Additionally, individuals or groups that take action to further the terrorist or narcotic organization's goals, which includes solicitation of financing or receipt of financing from foreign sources.

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 U.S., 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.

Incident Awareness and Assessment -- The use of intelligence, surveillance, and reconnaissance Department of Defense (DoD) intelligence capabilities for domestic, non-intelligence activities approved by the Secretary of Defense (SecDef), such as search and rescue (SAR), damage assessment, and situational awareness.

Intelligence Activity -- Refers to all activities that the Department of Intelligence (DoD) intelligence components are authorized to undertake pursuant to reference b. Note that reference b assigns the Services' intelligence components' responsibility for: 1, "Collection, production, dissemination of military and military related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking;" and 2, "Monitoring of the development, procurement, and management of tactical intelligence systems." This includes intelligence activities conducted by non-intelligence organizations.

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

Intelligence-related Activity -- Activities normally considered to be linked directly or indirectly to the intelligence field. Those 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 whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are 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 U.S., 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.

Memorandum of Agreement -- A document that defines general areas of responsibility agreement between two or more parties, normally headquarters or major command level components, that stipulates an amount of reimbursable cost -- what one party does depends on what the other party does (e.g., one party agrees to provide support if the other party provides the materials). 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 not depend on what the other party does (e.g., does not require reimbursement or other support from receiver). It may identify expectations of recurring support that normally are limited to short-term requirements not exceeding three years.

National Guard Bureau (NGB) -- The NGB is a joint activity of the Army National Guard (ARNG) and Air National Guard (ANG) pursuant to reference ee. The Chief of the NGB (CNGB) is under the authority, direction, and control of the Secretary of Defense (SecDef). The Secretary normally exercises authority, direction, and control through the Secretaries of the Army and the Air Force for matters pertaining to their responsibilities in law or Department of Defense

(DoD) policy. The CNGB is a principal advisor to the SecDef through the Chairman of the Joint Chiefs of Staff (CJCS) on matters involving non-federalized National Guard forces and through other DoD officials on matters as in reference ff or as determined by the SecDef.

National Guard Intelligence Component -- National Guard (NG) personnel conducting intelligence or intelligence-related activity. Intelligence personnel operating in both Title 10 and Title 32 status must comply with all federal Intelligence Oversight (IO) rules without exception. NG intelligence personnel operating in a state active duty (SAD) status are not members of the Department of Defense (DoD) intelligence component and are prohibited from engaging in a DoD intelligence or counterintelligence mission or using intelligence or counterintelligence (CI) systems, resources, or equipment, and, therefore, do not have to comply with federal IO policies. In SAD status, they are limited by state laws, to include state privacy laws. In most states, the collection, use, maintenance, and dissemination of information on a U.S. person is strictly regulated; therefore, NG members in an SAD status should seek competent legal advice on state laws before collecting information on a U.S. person.

Non-Reimbursable Support -- The cost of providing services that are within the mission of the host activity and are provided to all customers/tenants, regardless of use, and for which individual use cannot be accurately measured, should be budgeted by the host activity and provided to the customer/tenant on a non-reimbursable basis.

Necessary to the Conduct of a Function Assigned to the Collecting Component -
- For purposes of collection of information about a U.S. person pursuant to reference b, Procedure 2; this requires that the function be both an authorized intelligence activity (foreign intelligence or counterintelligence) and a mission delegated to that specific Department of Defense (DoD) 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 U.S., is not a U.S. person. A person or organization outside the U.S. is presumed not to be a U.S. person unless specific information to the contrary is obtained. An alien in the U.S. 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 Certifying Government Official that defines the organization's domestic imagery requirements and intended use. It also contains a proper use statement acknowledging awareness of the legal and policy restrictions regarding domestic imagery.

Proper Use Memorandum (PUM) Amendment -- The identification of and request for change to an approved PUM.

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.

Sensitive/Highly Sensitive Matter -- A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the Department of Defense (DoD) intelligence community or otherwise call into question the propriety of an intelligence activity.

Significant or Highly Sensitive Matter -- A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the Department of Defense (DoD) intelligence community or otherwise call into question the propriety of an intelligence activity.

Special Activities -- Activities conducted in support of national foreign policy objectives abroad that are planned and executed so the role of the U.S. 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.

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

United States Person Identifying Information -- A U.S. person is identified when his or her name, nickname, alias, unique title, Social Security number, or other unique personal identifier is revealed. 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.