UNCLASSIFIED

National Guard
Joint Force Headquarters State

Guide to Handling Information on U.S. Persons When Operating Within the United States

Pre-Decisional Coordinating Draft
V 1.1
23 Feb 10

UNCLASSIFIED

Purpose of the Handbook

The purpose of this handbook is to provide fundamental information on how JFHQ-States J2s can comply with the intelligence oversight program while conducting National Guard (NG) operations within the United States. This handbook will explain how to ensure mission accomplishment while protecting the constitutional rights and privacy of the U.S. population.

Many of the principles are based on the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO)'s program and Deputy Undersecretary of Defense for Policy (OSD-P)'s guidance. The handbook applies examples the JFHQ-State J2 is likely to encounter.

Applicability of the Handbook:

This handbook applies to the National Guard Joint Forces when in Title 32. It can be used as a base guidance document for the National Guard Service Component units when in T-32 but each service has additional guidance that should be considered. Though this handbook does reference State Active Duty, it is not intended to serve as a reference for that status. This handbook is meant to serve as a quick reference tool and is not meant as a substitute for the source documents. All JFHQ-States are responsible for knowledge of the original Directives.

This handbook is meant to serve as a quick reference tool and is not meant as a substitute for the source documents. All JFHQ-States are responsible to become familiar with the original Directives listed in the back of the handbook.

Objectives of the Handbook

This handbook has two main objectives:
First is the prevention of violations of the intelligence oversight programs and the protection of the statutory and constitutional rights of U.S. persons. Through the use of operational examples and lessons learned, the handbook attempts to increase the understanding of the activities that National Guard organizations and personnel may lawfully perform to accomplish their mission. Secondly, if prevention fails, the handbook outlines the process to identify, investigate, and report violations, and aggressively implement corrective actions to preclude recurrence.

Table of Contents

Section one: Intelligence Activities

APPLICABILITY

This section of the handbook applies to Title 32 National Guard Joint Intelligence activities. It is an overview of what constitutes intelligence and permissible National Guard intelligence activities.

Intelligence Oversight applies to all National Guard personnel and equipment when;

- □ Personnel are assigned or attached (temporarily or permanently) to units that perform intelligence activities regardless of specialty or job function.

or

- □ Equipment is used for the collection, production, and dissemination of intelligence regardless of unit of assignment. *or* equipment funding source.

***All National Guard equipment purchased by the National Foreign Intelligence Program is inherently intelligence equipment.*

The U.S. Intelligence Community

The Intelligence Community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. These activities include:

-Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;

-Production and dissemination of intelligence;

-Conduct of activities and collection of information to protect against, intelligence activities directed against the US, international terrorist and international narcotics activities, and other hostile activities directed against the US by foreign powers, organizations, persons, and their agents;

-Special activities;

-Administration and support of activities within the US and abroad necessary for the performance of authorized activities; and

-Such other intelligence activities as the President may direct from time to time.

The National Guard as a Member of the Intelligence Community

The National Guard is a member of DOD's intelligence community when conducting intelligence or counterintelligence activities to which part 2 of E.O. 12333 applies.

What makes something an intelligence activity? The community accepted definitions all include some type of predictive analysis.

Types of Intelligence

- **National Security Intelligence:** The Intelligence Community (IC) members conduct intelligence activities that are necessary for the conduct of foreign relations and the protection of the national security of the United States. As a DOD asset even when operating in T32, the National Guard is only authorized to conduct intelligence activities that are related to foreign intelligence and counterintelligence without further approvals. Like all National Guard operations, if it becomes necessary to support other activities, in this example an intelligence activity other than Foreign Intelligence (FI) or Counter Intelligence (CI), the National Guard command authority must consider the authority, status and funding prior to executing that support.

DOD Intelligence activities are defined as the collection, production, and dissemination of FI and CI. Without Secretary of Defense approval, DOD elements can only perform FI and CI activities that affect United States Persons.

* Foreign Intelligence: Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on the international terrorist activities.
* Counter Intelligence: Information gathered on activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. *(Source: DOD Reg 5240.1-R, December 1982)*

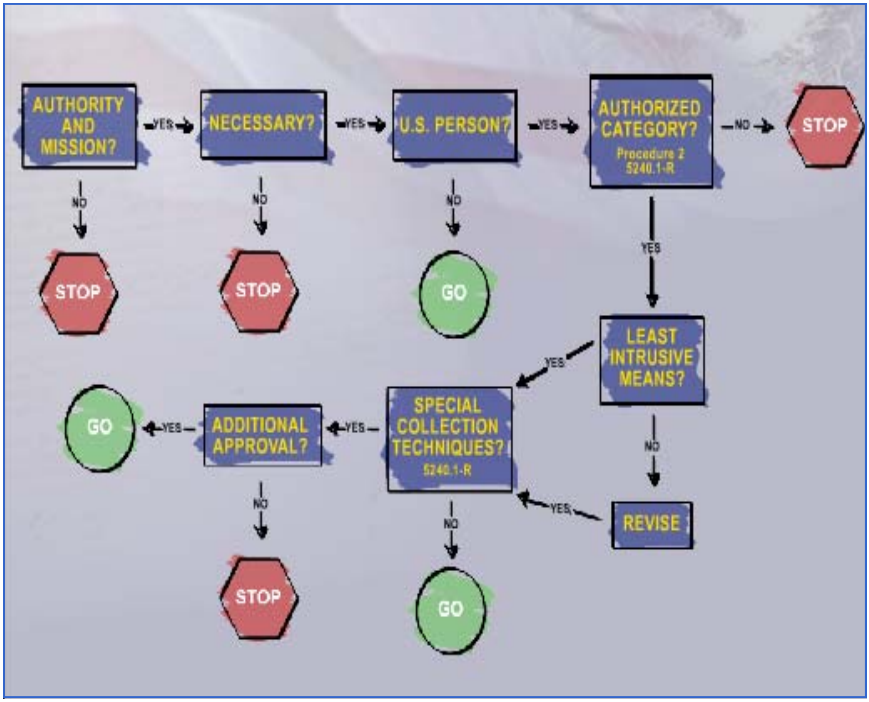
JFHQ-State J2s do not have an independent CI collection mission. National Guard units may support active component CI missions as regulated by DOD. Adjutants General will sign an understanding of the mission with the supported CI organization. (*DoD 5240.1-R, December 1982*)

☐ **Homeland Security Intelligence:** A subcategory of National Security Intelligence conducted by the Department of Homeland Security's Intelligence Enterprise. It consists of intelligence activities that are related to homeland security threats. Intelligence is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Homeland Security Department, at state, local, and tribal levels, in the private sector, and in the IC.

The link between HSI and the National Guard is so strong that in many states the Adjutant General is also the Director of Homeland Security. If asked to support a homeland security intelligence activity ALL National Guard assets must be keenly aware of their authority, status, funding and intent. In this regard the determination of compliance with IO guidance can be complex. For instance one must consider if there is a foreign nexus? Is it part of the element's METL? Is it within the purpose of the funding being used? Are the activities overt and transparent? And finally, have we properly safeguarded U.S. Person's information? For clarity the best approach is to request advice from the NGB J2.

☐ **Law Enforcement Intelligence:** Intelligence activities undertaken for the purpose of detecting violations of law or to locate and apprehend persons who violate the law. This includes activities to enforce the Uniform Code of Military Justice but there are very specific elements of DOD designated to perform Law Enforcement Agencies (LEA) intelligence. All DOD elements may cooperate with the LEA. However, the National Guard must never execute independent LEA intelligence activities nor assist LEA with intelligence tradecraft or resources without approval as explained in procedure 12. The National Guard can accept intelligence products of the LEA intelligence elements, especially when there is a direct and immediate threat to the National Guard and/or DOD mission, personnel, and facilities. Again the best approach is to request advice from the NGB-J2.

STEPS TO PROTECTING CIVIL RIGHTS AND PRIVACY



The flow chart above represents the decision process when considering how to handle U.S. Person's information during DOD's lawful intelligence activities as described in EO 12333 and DoD 5240.1. Each consideration is outlined in this section of the handbook. However, for a full explanation, consult the original source or your Senior Intelligence Officer, Inspector General or Staff Judge Advocate.

AUTHORITY AND MISSION

Specific Unit Mission

The first step to consider in working through the IO decision process is to consider each intelligence element's defined mission to determine permissibility to retain U.S. Person's information. Examples of sources of missions include EXORDS, OPORDS, USSIDs, EMAC, FEMA Mission Assignment or Secretary of Defense memorandums.

Example: In the case of the JFHQ-State J2s:

Mission: The Director JFHQ-State J2 advises TAG and Joint Forces Headquarters-State (JFHQ-State) staffs on all intelligence and security related matters that affect current and / or future NG operations. He is responsible for coordinating intelligence requirements for Joint Intelligence Preparation of the Operational Environment (JIPOE) in support of domestic and national missions. He serves as the executive agent for threat information sharing between local, state, and the national level to ensure situational understanding for a common operating picture (COP). Interprets, develops, and implements intelligence and security guidance and policy for the JFHQ-State.

Thus, the JFHQ-State-J2 directorate will provide accurate and timely warning of threats. How to analyze the threat is explained in the JIPOE Within the United States Handbook, but in general when considering the most likely (ex: weather related) and most dangerous (ex: foreign extremist WMD) it is highly unlikely you will need U.S. Person's information. Threat examples are contained in the list of all hazard threats.

Ask yourself, do you have the Authority and Mission:

☐ Is it a ***function of intelligence***? Ex: Yes, foreign terrorist analysis

AND

☐ Is it within my ***current mission authority***? Ex: Yes NG WMD disaster response mission as stated in your state emergency plan.

AND

☐ Does it ***Directly Support*** the TAG and JFHQ-State decision makers to allow for consideration of the widest range of options? Ex: CCIR/PIRs

- ***If the answer is No….Stop***

In the previous example , the most dangerous threat may indeed be a foreign extremist terrorist group planning a WMD assault within the state (JFHQ-State J2's area of responsibility). Therefore when thinking through the traditional JFHQ-State J2's responsibilities of providing assessment of foreign capabilities and intent, the J2 must consider:

Within the United States, foreign intelligence concerning United States persons may be collected only by overt means. This is true unless a specific set of conditions are met and then it must still be coordinated with the National Security Branch - the FBI, approved in writing by the head of the DOD intelligence component concerned, and then provided to the Deputy Under Secretary of Defense (Policy). The NGB J2 MUST be consulted prior to any active collection of foreign intelligence concerning US Persons.

JFHQ-State J2s do have the authority to use DOD information contained on SIPRnet and JWICs. Best practice is to use the IC derived information, redact all but the most necessary U.S. Person's data, and use general trends and observations in your assessments.

When trying to understand under what circumstances a JFHQ can collect U.S. Person's information you must understand what the mission and authority is to receive the information. For DOD, authority to conduct activities that affect U.S. Persons are derived from EX 12333 and relate to the National Security Intelligence Activities of FI and CI. This is not meant to imply they are the only Intelligence Activities in the U.S. IC, nor the only authorized intelligence function of a JFHQ-State J2.

JFHQ should not collect U.S. Person's information to perform other U.S. IC Intelligence Activities other than as permitted by DOD, which is FI or CI. At the Same time JFHQ-J2 are also not limited from performing other J2 functions such as Threat analysis, weather effects, strictly because it is not FI. Go for it, just Redact U.S. Person's information.

Common Pitfalls when applying authority:

Example one: Some JFHQs have attempted to avoid compliance by renaming missions as not being "an intelligence activity". For instance, in an eager effort to support LEA partners in a state fusion center the JFHQ tries to justify using DOD assets to analyze gang activity, do network diagramming or predictive analysis on their criminal behaviors. They do this by asserting that these are not intelligence activities because it is not Foreign Intelligence (FI) or Counterintelligence (CI) and that therefore IO does not apply. Renaming a mission will not legitimatize it.

Example two: Some JFHQs have applied a specific unit mission inappropriately. Some units have many unrelated missions that do not necessarily have the same authorities.
An example of this misapplication would be; citing a linguist or imagery sensor's authority from a counter narcotics mission as a specific unit mission function when they are used to support a non-narcotics related mission. So, if a local agency asks for the translation of documents belonging to a suspect detained for non -narcotics related crimes support may be permissible but would need separate approvals. The unit should take care to identify the correct source of authority to justify the current activity.

Now if you have determined you have the mission and authority you can move on through the next steps.

NECESSARY

Necessity: The question of necessity is again related to the unit mission and authority.

Is the proposed activity required to complete the National Guard's mission? Does the activity specifically support the Commander's Critical Information Requirements and Priority Intelligence Requirements? Is it necessary to make a decision or is it necessary to determine a course of action at a decisive point? Can you disregard the information or substitute the words "U.S. Person" and still complete the mission? If you answer "No-it is not necessary" then stop and remove the U.S. Person's information. Edit the non-relevant information. REDACT, REDACT, REDACT.

If the answer is "Yes-it is necessary" continue to follow the flow chart.
If the answer is, "I don't know" than try to determine in the most expeditious method possible but, you can retain the US Person's information during the determination period not to exceed 90 days. See "retention" within this section of the handbook.

Most JFHQ-State J2's threat assessments and intelligence reporting in support of specific National Guard Missions would NOT require collection of U.S. Person Information.

Examples of application of necessity:

On occasions, the National Guard is tasked to support the National Intelligence efforts such as that Congressionally approved in the Joint Reserve Intelligence Program or Counternarcotics Program. These types of missions may have exceptions allowing the use of U.S. Person's data.

When supporting other agencies: Each appropriately supported Federal Agency as well as CNGB and Adjutant General signs a letter of understanding of the mission guidelines and the limitations on National Guard support. Even during such operations, collection on U.S. Persons is often inadvertent and the necessity question is addressed by the supported Agency's lawful guidelines. If in doubt consult the supported agency's guidelines, your Staff Judge Advocate, Inspector General or Senior Intelligence Officer.

The National Guard's default is "no-it is not necessary".

Common Pitfalls when applying necessity

Example one: The NG provost marshal receives a "be on the look out" (BOLO) from the local police that a father is concerned for his son who has threatened employees at his local plant. The son is not in the NG and the plant is not located near the NG armories. The BOLO mentions that the son is expected to be going to the plant. In this example there is no reason to share this U.S. Person's information within the NG. There is no necessity to use the information. Despite the mission and authority to protect the force, there is no immediate and direct threat to the National Guard.

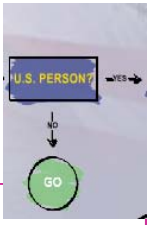
Common Pitfalls when applying necessity:

Example two: The JFHQ State receives a report from the local fusion center about the arrest of a local man with a homemade bomb in the trunk of his car. The fusion center noted that the bomb was unlike those of the past. The JFHQ is not familiar with the man arrested and can see no immediate need to retain his name since he is under police custody. The JFHQ J2 retained the U.S. Person's name because he wanted to address the new method of explosive in the modeling of possible blast effects. In this example he should have redacted the specifics of the U.S. Person but could keep the information on the explosive as a new terrorist method.

Example three: An inexperienced JFHQ-State J2 thought the monitoring of local criminal activities was necessary to complete the mission of the JFHQ-State as predictive analysis of local threats. Public safety (often state active duty or a specified mission of the NG during specific mission timeframes) and national security (federal missions including international terrorism, narcotics and foreign military activity) are not the same thing. The J2 wants to train to his JMETL and do JIPOE of his area of responsibility, his state. He can use the local intelligence threat assessments, that are shared with the NG, to understand the most likely and most dangerous threats. But should redact US Person info.

The more specific your state plan and the named mission for the National Guard, the more necessary some information may become but the J2 should not perform local law enforcement intelligence missions. In general, a generic "be prepared" for emergency response mission allows for a more generic threat assessment with general comments ("local gang activity is present") not specific analysis on local U.S. criminals (gangs named). Again most U.S. Person threat information is not deemed as necessary. Though some U.S. Person's non-threat information maybe necessary. See examples under the section, "Consent".

U.S. PERSONS



Defining U.S. Persons

- ☐ A U.S. Citizen

or

- ☐ A Permanent Resident Alien

or

- ☐ A U.S. Corporation not controlled by a Foreign Government

or

- ☐ An Association composed of mostly U.S. Citizens or Permanent Resident Aliens

(*DoD 5240.1-R,*)

Examples of application:

When considering applying the question of, "Is this a U.S. Person?":

- ☐ Person or organization known to be in the United States is presumed to be a U.S. Person unless specific information to the contrary is obtained such as a U.S. intelligence component or law enforcement agency has determined them to be otherwise. (*DoD 5240.1-R, appendix A-5*)

- ☐ Foreign national known to be in the United States is presumed not to be a U.S. Person / or permanent resident alien unless specific information to the contrary is obtained. (*DoD 5240.1-R appendix A-5,*)

- ☐ Person or organization known to be outside of the U.S. is presumed not to be a U.S. Person unless specific information to the contrary is obtained. (*DoD 5240.1-R,, page 5-7*)

AUTHORIZED CATEGORIES

Authorized Categories

There are certain categories of TYPES OF U.S. PERSON INFORMATION that may be used AFTER you determine that you have the mission and authority.

TYPES OF INFORMATION THAT MIGHT BE PERMISSIBLE TO COLLECT ABOUT U.S. PERSONS *(DoD 5240.1-R, procedure 2)*

Information that could identify a U.S. Person may ONLY be collected by a National Guard intelligence component if it is necessary to the conduct of an assigned function and it falls into one of these categories:

1. **Information obtained with consent**
2. **Publicly available information**
3. **Foreign Intelligence**
4. **Counterintelligence**
5. **Potential sources of assistance to intelligence activities**
6. **Protection of intelligence sources and methods**
7. **Physical Security**
8. **Personnel Security**
9. **Communications Security**
10. **Narcotics**
11. **Threats to Safety**
12. **Overhead Reconnaissance**
13. **Administrative Information**

Examples of Application of Category 1:

Category 1: Information obtained with consent: The agreement by a person or organization to permit DOD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure.

A few Examples:

- Often a public sector "U.S. Person" voluntarily consents to the NG analysis. The Guard has an evacuation mission under the state emergency management plan. A privately owned elderly care facility is identified as needing evacuation during disaster operations. The owner consents to the J2 including the facility in the intelligence preparation of the environment assessment products.

- During disaster response operations flooding event, there is a privately owned levy where the NG will reinforce with sandbags but the J2 needs to determine current water saturation levels. It is a J2 function to conduct the IPE assessments. The owner of the levy is permitting the National Guard to analyze the integrity of the levy.

- During an exercise the CI intelligence unit is performing CI METL tasks. A fellow Guardsman volunteers in writing to be covertly monitored during the training exercise.

Examples of Application of Category 2:

Category 2: Publicly available information: Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could be lawfully seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

A few examples:

- Before you use any publicly available information that identifies U.S. Persons, you must have a legitimate mission to do so. If you are working through this handbook step by step you have determined that you have a mission that requires an intelligence function, say you are the analyst conducting JIPOE of your AOR, the state. So the location of local private schools and churches that are listed as emergency shelters might be something you "collect" off the internet. The use of that information is limited and related to your mission and necessary purpose. If you have the mission, then collection of information on U.S. Persons that is publicly available is one of the thirteen categories of information that may be collected (see DoD Regulation 5240.1-R, Procedure 2). Any information that is legally collected by a DOD intelligence component may be retained and disseminated. Prudent application is to think that any use of U.S. Person's information should be kept to a minimum (risk adverse method). So, REDACT most U.S. Person's information from domestic and criminal threat reporting, especially if it is not foreign terrorist related. Also avoid all data based information that contains U.S. Person's info. However, it is a prudent use, if it is non-threat related information such as in this example.

Common Pitfalls for Category 2

A JFHQ thinks it can collect information on the local gangs because the information is available on the internet. Remember you must have a mission before you review the approved categories but it is not the National Guard's mission to conduct local public safety law enforcement intelligence activities. You do not have that mission thus even if publically available you can not collect without the national security threat nexus.
Another common mistake is often about the organization that has a lawful permit to publicly demonstrate against the government. A JFHQ wants to understand their position and opposition to the government. They ask the J2 or PM for any information about the group. The National Guard doesn't have any legal right to collect information on U.S. organizations that are not affiliated with the DOD and are no immediate or direct threat to the DOD. While the information maybe publically available there is still no mission authority. This group has a lawful right to oppose the government.

Examples of Application of Category 4:

Counterintelligence: (See definition page 6)

Examples: In preparing the NG leadership for a State Partnership Program (SPP) event, the JFHQ State J2 read an OSI country report indicating a named U.S. Person was involved in assisting another nation's sabotage in the SPP country. The third nation's best interest is to disrupt the U.S. and SPP partnership. In this example, the information is related to the mission and is an authorized category. It is permissible.

Examples of Application Category 12 :

The National Guard intelligence components may find it necessary to acquire collected or archived imagery to perform some T-32 missions. The National Guard use of domestic imagery (commercial, national and International satellite and airborne imagery sensors) must meet certain guidelines. National Guard can utilize the archived imagery on USGS servers and/or request imagery from NGA or FEMA with certain valid requirements. The purpose of the imagery will not be to obtain USPERS information or target USPERS private property. The use of the NG equipment such as Aerial sensors, WIDS, GIIEP and ROVERs may require a PUM (See additional approval section)

The JFHQ-J2 will:

- Submit completed "RFI Form for vetted National Guard Request" through JIEE to NGB J2 via NGB JoCC to include the following
  - Name of mission/event
  - Location(s) of the imagery requested
  - How the imagery will be used
  - Who the JFHQ-J2 will shared with
  - Justification for the imagery request
- Submit PUM with the RFI, if none were submitted before

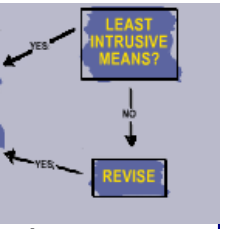
NGB J2 will:

- Validate the RFI
- Assign NGB Validation Number to the "RFI Form for vetted National Guard Request"
- Forward the JFHQ-J2's RFI form to NGA LNO

The JFHQ-J2 will:

- Upon receipt of the RFI products, JFHQ-J2 will provide feedback to NGB J2 on satisfactory of the products.

LEAST INTRUSIVE



Least Intrusive

(must be considered in this order)

☐ Is the information available **publicly or with the consent** of the person concerned?

☐ If not, can it be obtained from **cooperating sources**?

☐ If not, can it be obtained using other **lawful investigative techniques** that do not require a judicial warrant or the approval of the attorney general?

☐ If not, a judicial warrant or the **approval of the attorney general** may be sought.

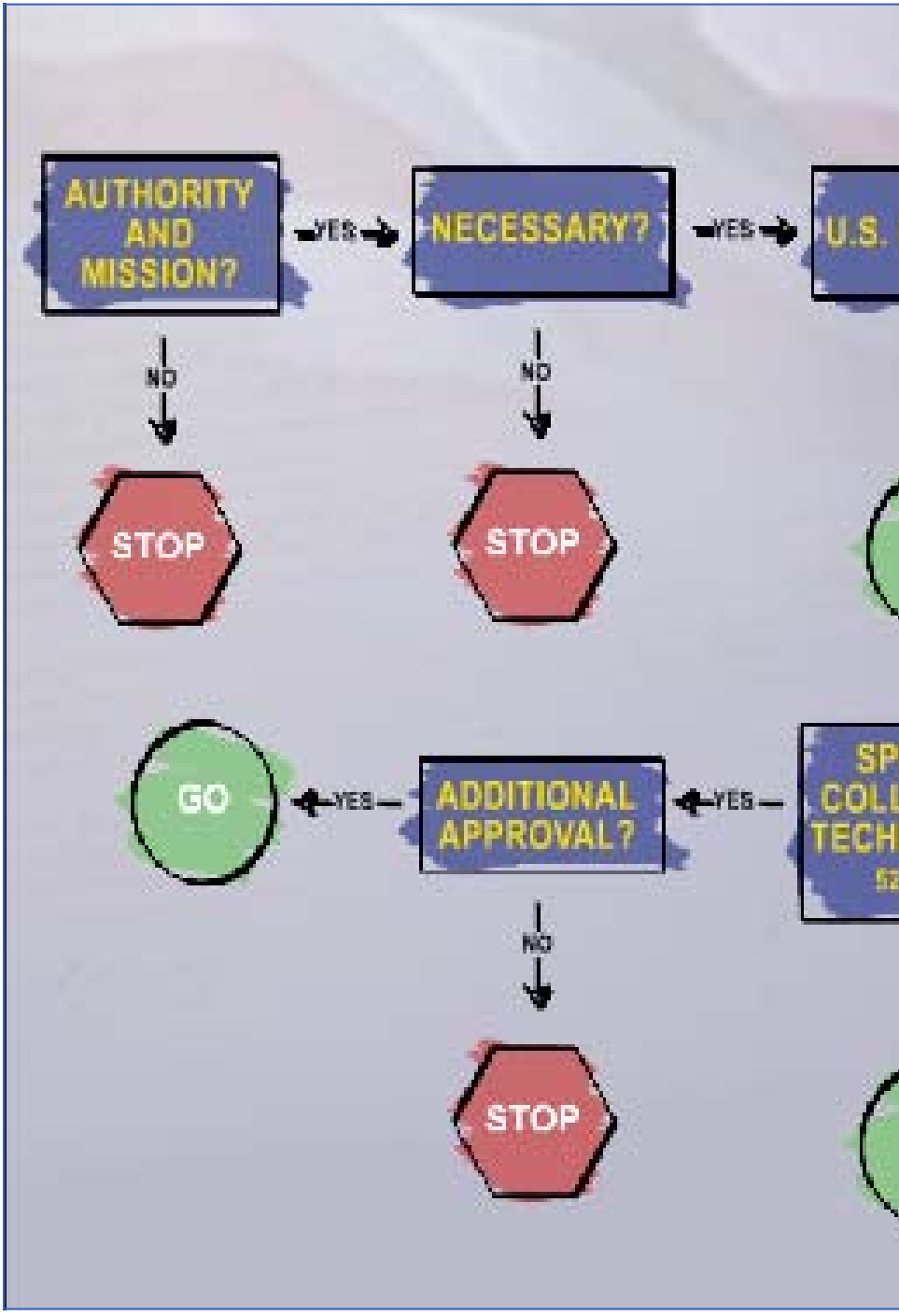
Least intrusive methods for JFHQ-State J2s include: monitoring intelligence reporting and the related open sources and coordination with the intelligence or law enforcement communities.

When related to US PERSON data, JFHQ-State J2s and JTF-J2s should avoid active collection but instead, JTF-J2s should process the event's information that is legally collected by the LEAs, Emergency Managers, or the responsible agency. Collect and retain only that information that best provides the information necessary for the mission. Such as threat information that is necessary for the TAG, JTF-CDR and other defense decision makers to consider the widest range of options. Take care to present the threat information that is relevant to the JFHQ-State and JTF missions and is the most timely, substantive, thorough, contextual, and useful in form and format.

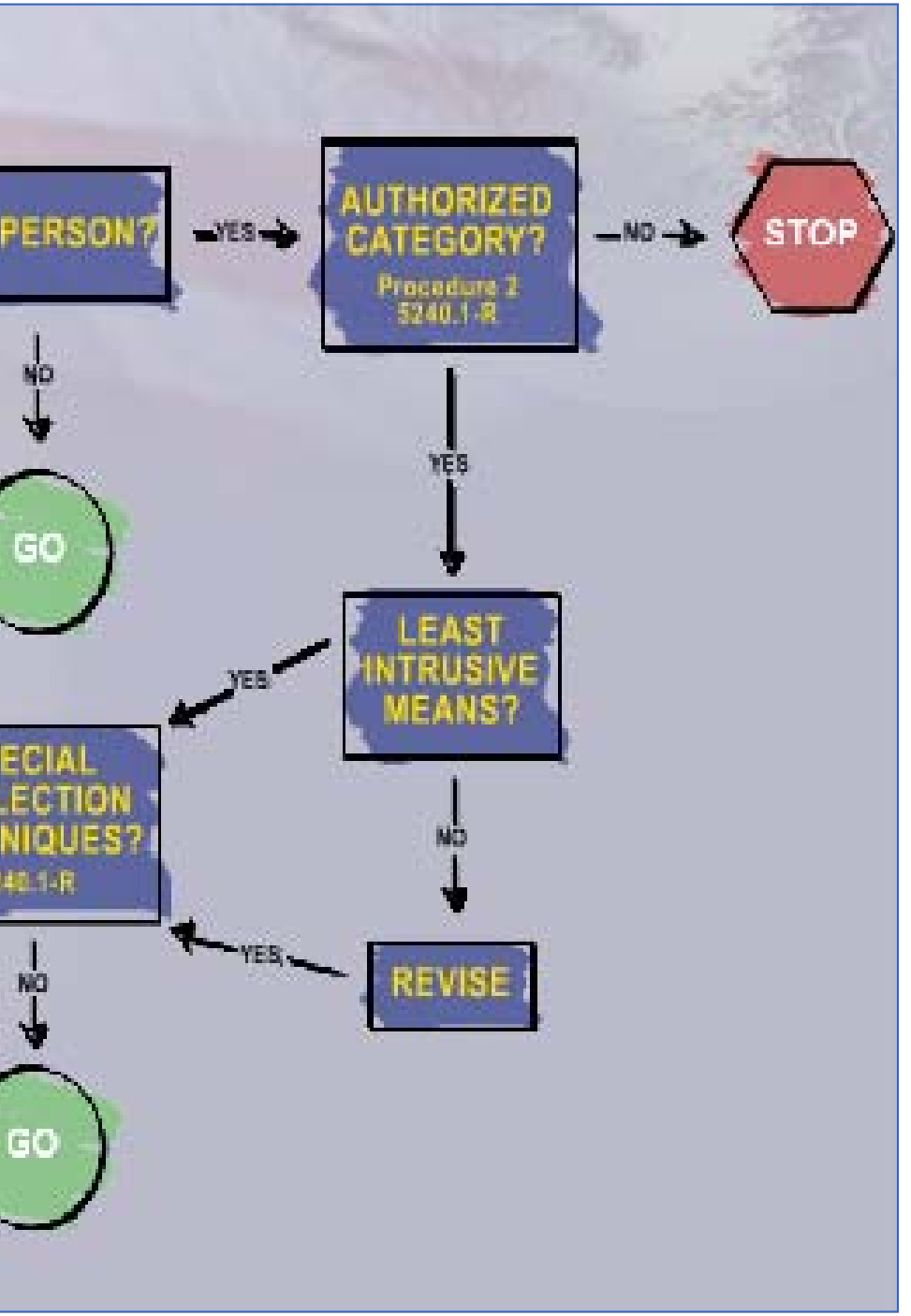
Common Pitfall:

Often J2s skip the first steps and jump straight to least intrusive. They fail to show the mission and authority to collect and justify obtaining the information just because it is publicly available and not intrusive. They obtain domestic extremist groups information because it is on the internet but cannot explain what national security mission they supported that required U.S. Person's information.

The Intelligence C



Oversight Process



Examples of Application of Least Intrusive:

Examples of Publically Available and With Consent are explained under the approved categories section. But when applying the Least Intrusive step the JFHQ-State J2 must think through the options to obtain the information and purposely take the method that is the least intrusive. An example: The National Guard is part of T-32 disaster response operation after a disaster caused by a large explosion. The National Guard has developed CCIRs and PIRs based on the need for information that impacts the NG operation. The J2 is considering his options. Step one: After a quick review of his mission and authority, he determines the NG has proper mission because of the EXORD signed by an appropriate authority. He also has the mission and authority to provide intelligence support to the operation as outlined in annex B. Step two: He determines the U.S. Person's information is necessary to understand the possibility of additional attacks. Step three: While a foreign terrorist group is claiming responsibility, the attacker is assumed to be a U.S. Person because he is currently within the U.S. and he is not known to be a foreign national. Step 4: The J2 realizes the information fits multiple categories under procedure 2. He assumes that because of the terrorist organization's claims, there maybe a tie to foreign intelligence and he can use information obtained by the U.S. IC. He also knows the forward units can report their observations of their checks of their perimeters for physical security purposes and he can also use information if there is a threat to the safety of the NG mission. Finally he knows the NG response force includes equipment that is capable of obtaining overhead reconnaissance imagery. Step five: This steps has him planning the information collection by the least intrusive method. The J2's plan should include information obtained by the least intrusive methods. The least intrusive is the LEA and IC reporting that is being shared with the JFHQ-State J2. He can also use news media reports and eyewitness testimony but the information that is broadcast on the news is not sufficient to answer the PIRs. However, tasking a remote sensor to take aerial photos is not the least intrusive if the information is already available by the lead agency.
Best response under the least intrusive step is the use of US IC products and LEA information obtained by federal, state and local authorities.

SPECIAL COLLECTION TECHNIQUES

COLLECTION: Information about U.S. persons is considered to be collected if it is received for use by an employee of the National Guard in the course of his official duties.

SPECIAL COLLECTION TECHNIQUES

ALL special collection activities of the National Guard's intelligence components must be coordinated through the NGB-J2 for approval by CNGB, SecDef and the U.S. Attorney General, even during emergency situations. Special collection activities include:

- 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

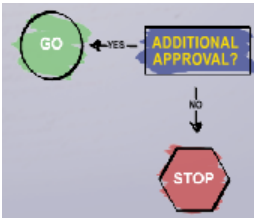
- Any other activities that could be perceived by the general public as a covert surveillance and covert reconnaissance activity (NGB-Policy).

(DoD 5240.1-R, procedure 5-11)

Some activities require additional approvals especially special collection techniques.

For the National Guard additional approval is often needed such as for the use of airborne imagery collection or intelligence support to a law enforcement activity by a military intelligence element.

ADDITIONAL APPROVALS



The Proper Use Memorandum (PUM)

A PUM provides details validating the legality of special collection techniques such as domestic airborne imagery activities conducted using National Guard aircraft. JFHQ-States that own or have operational control over National Guard aircraft operating in the CONUS are responsible to generate a PUM. JFHQ-State will submit PUMs for all Title-32 missions that include the collection of imagery within CONUS prior to the execution of a mission.

The primary purpose of the PUM is to protect and explain the valid reasons behind military activities and to ensure that the rights of United States citizens and organizations are also being protected in accordance with the law. The PUM ultimately communicates the intent of military activities and justifies that those activities are not violating or imposing upon those constitutional rights.

All National Guard PUMs will be submitted through NGB-J2 to be forwarded to the appropriate Office of General Counsel for review.

Electronic Templates of PUMS are available for download on the NGB J2 Community of Practices located on the J2 Guard Knowledge On-line.

If the activity is non-intelligence than a PUM is not required but a Request for Technical Assistance (RTA) might be...refer questions to the NGB-J2.

Common Pitfalls:

- To assume that federal statutes and guidance are more restrictive than state laws. Senior Intelligence Officers must consult with their JFHQ-State SJA when performing as a J2 in State Active Duty.
- To Use a National Guard counterdrug asset for a non-counterdrug mission without completing a PUM or RTA memo.

Military Intelligence Components Cooperation with Law Enforcement Authorities:
Often referred to as Procedure 12, National Guard intelligence components are authorized to cooperate with LEAs for the purposes of:

□ Investigating or preventing; clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

or

□ Protecting DoD employees, information, property, and facilities;

or

□ Preventing, detecting, or investigating other violations of law.

Types of Permissible Assistance:
□ Incidentally acquired information reasonably believed to indicate a violation of Federal law

or

□ Incidentally acquired information reasonably believed to indicate a violation of State, local, or foreign law

or

□ Personnel or specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law enforcement authorities, ***provided such assistance is consistent with DODD 5525.5, has been approved by NGB-J2,*** and that the NGB-JA concurs in such use.

(*DoD 5240.1-R, procedure 12*)

The Procedure 12 Memo provides details validating the legality of providing National Guard intelligence component's personnel, specialized equipment, or facilities to law enforcement authorities when they are used to support intelligence functions of those agencies. JFHQ-State will generate a P12 Memo as required and will seek approval through proper channels prior to the execution of a mission.

Electronic Templates of P12 memo are available for download on the NGB J2 Community of Practices located on the J2 Intelink site: https://intelink.gov/sites/ngb-j2

Examples of Application:

- Lead Federal Agency Request to use the National Guard's SIPRNET or JWICS during a National Special Security Event.

- A request for assistance to use a linguist, regardless of military occupation or duty code, to assist in a Law Enforcement Agency intelligence analysis element. (LEA Intel Activity)

- A request for assistance to use a intelligence linguist to assist in a Law Enforcement Agency investigation. (LEA Non-Intel Activity)

Common Pitfalls:

- JFHQ-State J2 fails to obtain concurrence from their Staff Judge Advocate when the LEA support includes personnel used as expert advisors or operators and maintenance for equipment.

- JFHQ-State support to local and state LEA when lives are not endangered.

- JFHQ-State J2 fails to document the approval of the support in a procedure 12 memorandum.

DISPOSITION OF INFORMATION

RETENTION: U.S. Person's information may be retained if it was collected pursuant to Procedure 2 DoD 5240.1-R, December 1982. The information will be retained according to the archivist of the United States. For example: Some operational files are retained for 3 years and some for 10 years.

Incidental Acquisition: If the information is acquired incidentally:

- ☐ It can be retained IAW mission if information could have been collected intentionally under Procedure 2
- ☐ It can be retained temporarily if:
  - ☐ determining whether that information may be permanently retained
  - ☐ for a period not to exceed 90 days
  - ☐ only as necessary to transmit or deliver such information to the appropriate recipients. (See section on dissemination)

It can be retained temporarily if: determining whether that information may be permanently retained for a period not to exceed 90 days and only as necessary to transmit or deliver such information to the appropriate recipients. (See section on dissemination). The 90 days is an exception to determine not an exception to retain. So if it is determined that the information should not be retained, it should be purged, destroyed, or provided to the appropriate agencies immediately. If it is determined that the information was collected pursuant to Procedure 2 DoD 5240.1-R, December 1982, then it should be retained in accordance with the guidance of the Archivist of the United States (i.e. as permissible for that mission, commonly 2-3 years for operational files.)

Common Pitfalls when applying retention:

Example one: Retaining information for up to 90 days even after it has been determined to be U.S. Persons and that it could not have been collected pursuant to Procedure 2 *DoD 5240.1-R, December 1982*. The 90 days is not an exception to "retain", it is an exception to "determine" .

Example Two: Retain information that is not the National Guard's.

- If the mission is in support of another agency: Once the mission has been concluded, all collected information is purged, destroyed, or provided to the appropriate agencies in accordance with applicable regulations and laws.
- If the information was obtained for a mission that is not an intelligence activity thus was not collected pursuant to Procedure 2, DOD 5240.1-R, Dec 1982, then the information on U.S. Persons should be purged, destroyed, or provided to the appropriate agencies in accordance with applicable regulations and laws associated with that type of mission.

Example Three: Obtaining information properly but then creating a database for other uses of the information.

DISSEMINATION: For the performance of a lawful governmental function, U.S. Person's information can be shared with:

- ☐ An employee of the DOD with a need for such information in the course of his or her official duties;

or

- ☐ A law enforcement entity of Federal, State, or local government, if the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;

or

- ☐ An Agency within the intelligence community to determine whether the information is relevant to its responsibilities. It is the responsibility of that Agency to determine relevancy. The National Guard will not be responsible to make that determination and will not retain the information after it is shared with the other intelligence agency.

Access to retained information is limited to those with a need to know. JFHQ-State J2s should only retain and/or disseminate the minimum information necessary to perform the mission.

Release of Information to the Public:
It is the primary responsibility of the civilian agency that is the lead for performing the lawful government function to release information to the general public. The National Guard will not, to the extent possible, release information on persons not in the National Guard without consulting the affected civilian agency.

Employee Conduct

All National Guard TAGs, Directors JFHQ-State, Senior Intelligence Officers, and J2s are responsible to ensure all intelligence components are familiar with statutory and regulatory guidance (listed on page 37 of the handbook) to include all restrictions and reporting responsibilities.

All employees of National Guard Joint intelligence components will conduct themselves according to all statutory and regulatory guidelines and will not exceed the authorities granted to them. All employees are responsible to report any intelligence activity that they suspect may violate the guiding laws or policies.

Each employee is obligated to report any intelligence activity that they suspect may violate the laws or policies to the JFHQ-State J2, Senior Intelligence Officer, State Judge Advocate or Inspector General. *(DoD 5240.1-R, December 1982 procedures 14 and 15*)

Reporting Questionable Activities

- Report questionable intelligence or operational activities
- "Questionable Activities" are those constituting or relating to a National Guard activity that may violate the law
- Report "Questionable Activities" through your chain of command, IG, General Council, JAG, IO officer or higher levels. Whistle blowers are protected from retribution or adverse action

Attributes of a Good Intelligence Oversight Program

Effective Training
Periodic Refreshers
Documented program, processes, and training
Spot checks
Tailored to Unit and mission

Conducting non-intelligence Support Operations

Cooperating with Civilian Agencies:

It is the National Guard policy to cooperate with civilian government officials to the extent possible while protecting the statutory and constitutional rights of U.S. Persons.

The National Guard is encouraged to share any information collected during the normal course of military operations that maybe relevant to Federal, State, Local, or Tribal government agencies if it falls within their lawful government function, within their jurisdiction, and is consistent with national security policies.

This section discusses the collection and sharing of information on persons not in the National Guard. It is not intended to address authority to conduct missions in support of civilian agencies. All requests for assistance should be directed to the NGB JOCC or JFHQ-State J3.

Questions about the evaluation of requests for assistance other than about handling information on U.S. Persons and Non-DOD affiliated persons should be directed to the NGB J3, SJA, or IG.

(DoD Directive 5525.5 and NGB Policies)

Emergency response authority :

□ Under the emergency authority, the National Guard is often used to support civilian authorities to safeguard life, property and public order. During such emergency situations the National Guard is authorized to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disaster, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situation.

TAG, when, in his judgment, the emergency is direct and immediate and time precludes obtaining prior approval may authorize support activates that include lawful acquisition of U.S. Person's information when that support is consistent with the Constitution and other legal rights of U.S. persons.

The JFHQ-State must implement the proper safeguards to protect all information and products collected, acquired, received or used during the emergency response and ensure all applicable security regulations and guidelines, and other restrictions will be followed.

In each such case a report will be made immediately to the CNGB through the NGB- JOCC.

Whenever National Guard personnel, equipment and facilities are used to support civilian agencies, handling US person restrictions should always be kept in mind. Due to the potential legal pitfalls, aiding civilian agencies in non-emergency situations should be avoided. As a rule, your JAG officer should be consulted prior to providing any support to civilian agencies.

Incident Awareness and Assessment Authority :

National Guard personnel and equipment can be used for Incident Awareness and Assessment (IAA) to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disaster, or calamities seriously endanger life and property and disrupt normal governmental functions but only upon receipt of a JFHQ-State or NGB validated Government Agency's Request for Assistance (RFA). The Agency must be operating within its lawful function and authority, such as; at the request of the Governor's Office, the Primary or Lead State or Federal Agency for the event, an EMAC request, or a Mission Assignment (MA) from FEMA.

Under the conditions stated above, TAGs are authorized to utilize NG (both intelligence and non-intelligence) component capabilities for non-intelligence activities to provide aerial imagery sensor platforms and technical support to federal, state, and local agencies, for IAA, to include damage assessment, search and rescue, evacuation monitoring, situational awareness and CBRNE assessment in support of disaster relief operations in the affected areas.

Authorized NG intelligence component capabilities for non-intelligence activities include:

☐ The analysis of imagery, geospatial data, and information collected from cameras, video, electronic optics, IR and FLIR, and the dissemination of final products based on that analysis.

☐ The analysis of information collected from government agencies operating within their lawful functions and authorities.

☐ IAA to obtain baseline imagery for operational planning to determine probable landfall and post-landfall damage and to assess the severity of damage from hurricanes.

Example of Application: Information Shared with the National Guard from a Law Enforcement Agency

Without mission approval to assist Law Enforcement, information containing U.S. Person's information regarding criminal activities, gangs, armed civilians, congregations of civilians, looting, which does not indicate a direct threat to DOD forces, facilities, or operations will be passed to appropriate Federal, State, or Local law enforcement agencies (LEAs) and will not be retained by National Guard personnel.

National Guard is authorized collection of information about gangs, armed civilians or looting permitted only when a DIRECT threat to DOD or the unit is assigned missions in support of law enforcement that require the information.

The National Guard is authorized to receive information about gangs, armed civilians or looting if there is no specific U.S. Person's information, or if the NG can redact the U.S. Person's information, even if there is no direct threat to the National Guard, but the LEA or IC agency has included the information in threat summaries or intelligence products AND that non-specific information is necessary to conduct a NG mission. For instance a State fusion center's intelligence product includes information on a new technique of an IED by a US white supremacy group. The JFHQ-State J2 can refer to the new method of making the explosive but redact the specific group information.

When the National Guard unit's specified mission is security operations in support of a law enforcement mission, all information obtained on persons and organizations not affiliated with DOD, that does not indicate a direct threat to DOD forces, facilities, or operations, will be treated as the supported LEA's information. It will not be further 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, in accordance with applicable regulations and laws, once the National Guard mission has been concluded.

With the approval of the Secretary of Defense, aerial platforms and technology, such as cameras, video, electronic optics, IR and FLIR may be used to detect direct threats to DOD forces, facilities, and operations. Information obtained on persons and organizations not affiliated with DOD which does not indicate a direct threat to DOD forces, facilities, or operations will not be retained, but may be passed to LEAs.

Technology, such as cameras, video, electronic optics, 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 obtained on persons and organizations not affiliated with DOD which does not indicate a direct threat to DOD forces, facilities, or operations will not be retained, but may be passed to LEAs.

There are limits on the use of IC capabilities to support civilian law enforcement. Any requests for intelligence support to LEAs must be separately staffed and approved prior to mission execution. NG IC components may not task, direct, or request missions in direct support of law enforcement, unless authorized in accordance with DoD 5240.1-R, Procedure 12, and DoDD 5525.5 by the Secretary of Defense. See the earlier section of this handbook.

NG IC components are limited on the ability to task, direct, or request missions in direct support of DOD Title 32 force protection requirements or conduct threat analysis of domestic threats to Title 32 DOD forces **that is not** obtained through operational channels. Collection of information about gangs, armed civilians or looting is authorized only when a DIRECT threat to DOD **or the unit is assigned a security operation in support of law enforcement.**

Operations Related to Civil Disturbance.

If the National Guard is lawfully participating in a Military Assistance To Civil Disturbance Mission, information on non-DOD affiliated persons and organizations may be acquired if it is essential to meet operational requirements. The National Guard participation in such activities will only be permitted when there is a distinct threat of a civil disturbance that exceeds the law enforcement capabilities of State and local authorities.

Summary

U.S. Person information can be collected during an ***intelligence activity*** but only ***IF***:

- ☐ ***It is necessary to the conduct of a function*** assigned to the collecting component,

AND

- ☐ It ***falls within one of the approved categories***

AND

- ☐ It is obtained by the ***least intrusive*** means

AND

- ☐ It is obtained IAW Executive Order 12333.

(DoD 5240.1-R,)

U.S. Person information can be collected during a ***Non-intelligence activity*** but only ***IF***:

- ☐ ***It is necessary*** to the accomplishment of the DOD mission.

AND

- ☐ It is subject to civilian control, ***high level of supervision and frequent inspections.***

AND

- ☐ It is obtained by ***maximum reliance on domestic civil investigative*** agencies, Federal, State and local.

AND

- ☐ Limited to information essential to the protection of DOD functions and Property (Direct and immediate threats); Personnel Security programs (Investigations related to employment) or Operations relating to Civil Disturbance.

(DoD Directive 5200.27)

Prohibited Activities

The following activities are always prohibited:

☐ No information shall be acquired about a person or organization solely because of lawful opposition to Government policy.

☐ There shall be no physical or electronic surveillance of Federal, State, or local officials or of candidates for such offices.

☐ There shall be no electronic surveillance of any individual or organization, except as authorized by law.

☐ There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations.

☐ No National Guard personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information.

An exception to this policy may be made by TAG, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a report will be made immediately to the CNGB .

☐ No computerized data banks shall be maintained relating to individuals or organizations not affiliated with the Department of Defense.

No computerized data banks shall be maintained relating to individuals or organizations not affiliated with DOD, unless authorized by the Secretary of Defense through the CNGB.

List of References:

- Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended July 31, 2008 and by Executive Order 13284, January 23, 2003, Executive Order 13355, August 27, 2004

- Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005

- DoD Directive 5240.1, "DoD Intelligence Activities," Aug, 2007

- DoD Directive 5240.1R "Procedures Governing DoD Intelligence Component Activities," Dec, 1982

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

- DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials, " January 15, 1986 incorporating Change 1, December 20, 1989

- DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007

Service Specific References:

- AFI 14-104, Oversight of Intelligence Activities, 16 Apr 2005
- AR 381-10, US Army Intelligence Activities, 3 May 2007
- AR 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations, 20 Sep 1974
- AR 525-13, Antiterrorism, 4 Jan 2002

Release of Information to the Public:
It is the primary responsibility of the civilian agency that is the lead for performing the lawful government function to release information to the general public. The National Guard will not, to the extent possible, release information on persons not in the National Guard without consulting the affected civilian agency.

Available Templates

The following can be downloaded from the NGB J2 Community of Practice homepage, via intelink.

Requests for Assistance
Appointment Letters
Proper Use Memorandums
Procedure 12 requests
Exception to Policy

Useful Links:

Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) http://www.defenselink.mil/atsdio

Joint Intelligence Directorate, National Guard Bureau, NGB-J2
https://intelink.gov/sites/ngb-j2/default.aspx
https://secure.intelink.ic.gov/sites/ngbj2

Office of the Chief Counsel, National Guard Bureau, NGB-JA
https://gkoportal.ngb.army.mil/sites/NGB-SpecialStaff/JA/default.aspx

Office of the Provost Marshal, National Guard Bureau, NGB-PM
https://gkoportal.ngb.army.mil/sites/NGB-SpecialStaff/PM/default.aspx

Office of the Inspector General, National Guard Bureau, NGB-IG
https://gkoportal.ngb.army.mil/sites/NGB_IG/default.aspx

POC information

JFHQ-State J2s are encouraged to consult with the JFHQ-State Staff Judge Advocate for advice on compliance with law, policy, assisting local law enforcement and intelligence oversight. They should work closely with the SJA and Inspector General within the State.

NGB-J2: 703-607-1822
NGB JOC J2: 703-607-8725
NGB Inspector General: 703-607-2511
NGB-SJA: 703-607-2706
NGB-PM: 703-607-8730

National Guard Bureau
Director for Intelligence

NGB-J25
Intelligence Plans, Policy and Programs Division

1411 Jefferson Davis Highway
Arlington, VA 22202-3231
Telephone: (703) 607-8736