DEPARTMENT OF THE ARMY AND THE AIR FORCE
NATIONAL GUARD BUREAU
1411 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202-3231

18 JUN 2008

NGB-J2

MEMORANDUM FOR THE ADJUTANTS GENERAL OF ALL STATES, PUERTO RICO, THE U.S. VIRGIN ISLANDS, GUAM, AND THE COMMANDING GENERAL OF THE DISTRICT OF COLUMBIA

SUBJECT: (All States Log Number P08-0004) NGB Policy for Handling of U.S. Persons Information

1. References:

a. The Privacy Act of 1974, Title 5, United States Code, Appendix 552a

b. AR 380-13, 20 Sep 1974, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations

c. DoDD 5200.27, Jan 1980, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

d. Executive Order 12333, 4 Dec 1981, Intelligence Activities

e. DoD Directive 5240.1-R, Dec 1982, Procedure Governing the Activities of DoD Intelligence Components That Affect U.S. Persons

f. NGR 500-2/ANGI 10-801, 31 March 2000, NGB National Guard Counterdrug Support

g. AR 525-13, 4 Jan 2002, Antiterrorism

h. DoD O-2000.12-H DoD, 9 February 2004, Antiterrorism Handbook

i. AFI 14-104, 16 Apr 2005, Oversight of Intelligence Activities

j. CNGB memorandum, 29 Jun 2005, SUBJECT: Intelligence Oversight, posted on NGB-J2 GKO main page, general section

k. The Economy Act, 2 Jan 2006, Title 31, United States Code, Section 1535

l. This memorandum rescinds NGB-J2 memorandum dated 19 Jun 2006, subject: Intelligence Oversight in the Conduct of the JFHQ-S J2 mission.

m. AR 381-10, 3 May 2007, US Army Intelligence Activities

n. DoD Directive 5240.01, 27 Aug 2007, DoD Intelligence Activities

o. Chief of the National Guard Bureau (CNGB) Memorandum, 25 Mar 2008, SUBJECT: Intelligence Oversight, posted on NGB-J2 GKO main page, general section

2. Mission statement for State J2: 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. Responsible for coordinating intelligence requirements for Intelligence Preparation of the Environment (IPE) in support of domestic and national missions. Serves as the executive agent for threat information sharing between local, state, and the national level to ensure situational awareness for a common operating picture (COP). Interprets, develops, and implements intelligence and security guidance and policy for the JFHQ-State.

3. Restrictions for National Guard (NG) personnel:

a. NG personnel are not authorized to be involved in any direct collection activity concerning U.S. Persons.

b. NG personnel are not authorized to conduct any type of surveillance, "undercover" type operations, or counterintelligence activity.

4. Applicability

a. This policy memo applies to all members of the NG serving in either Title 10 or 32 statuses who handle information regarding United States Persons (USPERS) (see definition below). There are two main categories of information. The first involves USPERS Information that is collected by DoD Intelligence Components and is therefore governed by Intelligence Oversight Rules (references 1d, n, g, m and b) is located in Section 6. The second is information collected on Non-DoD-affiliated Persons and Organizations which applies to everyone in DoD EXCEPT Intelligence Components and is governed by DoD Directive 5200.27 (at reference 1b and 1f), and is provided in Section 7.

b. The NGB J2 Directorate is the primary proponent for this Joint Policy in coordination with the J2 Functional Area Council (FAC), NGB-J34, Inspector General (IG) and Judge Advocate (JA) representatives.

c. The NGB and State JFHQ - PM/J34 provides National Guard leadership with information and recommendations to assist decision-making pertaining to FP, AT Critical Infrastructure, Security and Law Enforcement (LE) activities. This is accomplished through review, analysis, and distribution of law enforcement threat information that is significant and relevant to the NG mission, personnel, infrastructure, and current or future missions for a domestic LE threat information capability. Assists with intelligence oversight requirements.

5. Definitions.

a. USPERS are defined as U.S. citizens, permanent resident aliens, unincorporated associations substantially composed of U.S. citizens or permanent resident aliens (e.g. Groups), and corporations incorporated in the U.S. and not directed or controlled by a foreign government. Some examples of USPERS information include:

(1) Name (individual, Group, or Corporation)

(2) SSN or Driver's License Number

(3) Phone Number

(4) Address or photograph/imagery that can identify the US Person

(5) Physical Description

(6) License Plate Number

(7) Date of Birth / Place of Birth

(8) Other information that can specifically identify a US Person.

b. Foreign Nexus is defined as reasonable evidence of ties to foreign powers, individuals or organizations, including international terrorist or narcotics activities through direct communications with other members, membership and or training in a terrorist organization, and declaration of allegiance to and adoption of terrorist ideology. Additionally, this includes individuals or groups that take action that furthers the organization's goals to include solicitation of financing or receipt of financing from foreign sources.

c. Collection, as defined, in DoD Directive 5240.1-R (ref 1e): Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. "Use" is defined as physically retaining information and producing a presentation or Intelligence Summary (INTSUM) containing data. Thus, information volunteered to DoD intelligence

component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. To further clarify, (ref 1o) information is collected when action is taken that demonstrates intent to use or retain the information for intelligence purposes (e.g. INTSUM, Threat Summary, Intelligence presentation, etc). J2 personnel may collect information to prepare intelligence products that either contain no USPERS data or USPERS data that has a verified foreign nexus. Verification can be achieved via the Federal Bureau of Investigations (FBI) as the lead federal agency for Counterterrorism in CONUS or NGB-J2.

d. Open Source Information. Intelligence Oversight also applies to Open Source and publicly available information. NG intelligence personnel are not authorized to specifically search for USPERS using public available media, nor initialize internet "search engines" to purposely target USPERS unless it is authorized function and the information falls within one of 13 categories specified in DoD 5240.1-R, Procedure 2. If threat or criminal information that contains USPERS is incidentally obtained from open sources, it should immediately be passed to the appropriate civilian or military law enforcement or DoD Anti-Terrorism /Force Protection section.

6. U.S. Person Information Subject to Intelligence Oversight

a. Intelligence Oversight (IO) requirements limit the collection, retention and dissemination of information on USPERS to specific exceptions related to foreign intelligence, international terrorist activities, international narcotics activities, to protect the safety of a person or organization, or information from overhead reconnaissance not directed at specific USPERS, if these exceptions are an assigned mission. IO prevents the unfettered collection of information regarding USPERS by the intelligence community. Within the DoD it applies to the DoD intelligence components. The collection of USPERS information by intelligence components will only occur when there is a specific mission and authority to do so. The NG does not have a mission to collect on USPERS, nor does it have a mission to perform counter-intelligence operations in CONUS in T32 status.

b. Intelligence Oversight applies to all members of the DoD intelligence community. DoD intelligence personnel engaged in any intelligence activity (e.g. collection, research, analysis, production, retention, or dissemination), as well as all non-intelligence personnel assigned to a DoD intelligence unit. All must be familiar with the provisions of EO 12333, DoD Regulation 5240.1-R, and their respective DoD component's specific Intelligence Oversight regulations and instruction. Contractors or non-intelligence personnel assisting in the performance of intelligence or counterintelligence work for DoD intelligence or counterintelligence organizations have the same IO responsibilities as government civilian and military personnel. They should receive the same training provided to government civilian and military personnel.

c. National Guard intelligence personnel operating in both Title 10 and Title 32 status must comply with all federal IO rules without exception. Questions regarding your authority while in a Title 32 status should be discussed with your State Judge Advocate (JA). NG intelligence personnel operating in a State Active Duty (SAD) status are not members of the DoD intelligence community; however they are limited by their State laws to include state privacy laws and are prohibited from engaging in what would be a DoD intelligence or counterintelligence mission while in a SAD status. SAD can not be used as a subterfuge to collect on USPERS that would be prohibited from collection in either T10 or T32 status. In most states the collection, use, maintenance and dissemination of information related to individuals by state agencies is strictly regulated therefore, practically speaking, even in a SAD status NG members can not collect information on USPERS. It is advised that State J2s consult with their JA in reference to their state laws regarding USPERS information.

d. State Active Duty personnel are prohibited from using DoD intelligence resources and DoD equipment while in a SAD status. National Guard personnel in a SAD status are being paid by the state and not considered to be functioning in a DoD capacity therefore they are not authorized to engage in DoD intelligence operations nor access DoD systems (SIPRnet / Joint Worldwide Intelligence Communication System (JWICS)) or equipment (MQ-1, border sensors) for a SAD mission without authorization from the NGB J2. States may re-assign intelligence personnel to a non-intelligence mission while in a SAD as long as they do not use or attempt to perform strictly intelligence functions.

e. The National Guard generally does not conduct domestic intelligence operations. Domestic intelligence involving USPERS is a law enforcement matter and is the responsibly of State or local LE agencies and the FBI. However, JFHQ-State J2 is the subject matter expert and advisor to the The Adjutant General (TAG) and JFHQ-State Staffs on all intelligence and security related matters. The JFHQ-State J2 is responsible for coordinating intelligence requirements for IPE in support of state and federal missions. The J2 serves as the lead proponent for foreign threat information sharing between local, state, and federal agencies to ensure situational awareness for a common operating picture (COP). The J2 also interprets, develops, and implements intelligence and security guidance and policy for the JFHQ-State. The State Provost Marshal (PM) / J34 serves as the lead proponent for domestic threat information sharing between local, state, tribal and federal agencies to ensure situational awareness for a COP. The J2, J34, and PM must work together, each contributing essential threat information, to ensure a complete COP is maintained within each state Joint Operation Center (JOC).

It is imperative that each state have organized and trained J2 sections that are Military Occupational Specialty (MOS) and Air Force Specialty Code (AFSC) qualified personnel with the appropriate security clearances. Likewise, it is equally important that these

sections work in conjunction with MOS and AFSC qualified and cleared PM/J34 or LE personnel to provide maximum coverage and awareness to enable the National Guard to respond to threats within the United States. The J2 advises the TAG and JFHQ-State to include staff members on all Intelligence Functional Areas. This includes current foreign related intelligence, intelligence policy, programs and special security operations in support of the Global War on Terrorism, National Special Security Events, Homeland Defense and Homeland Security missions. The National Guard J2 plays a critical role in developing the overall situational picture and ensuring intelligence personnel are fully trained and operational at the state level. Additionally, each JFHQ-State having trained and operational J2's enhances NG relations with other DoD intelligence components.

7. Information collected on Non-DoD-affiliated Persons and Organizations by members of the National Guard not serving in intelligence positions.

a. References 1b and 1f outline the handling requirements for sensitive USPERS information by other personnel who are not part of the JFHQ-State J2 staff or members of a DoD Intelligence Activity. The regulations are similar to Intelligence Oversight guidelines and regulations for intelligence personnel, but apply only to personnel that are neither assigned to JFHQ-State J2 functions nor possess an intelligence MOS or AFSC and are referred to here as non-intelligence (non-MI) personnel. Non-MI personnel cannot be used to collect information on USPERS or "by pass" intelligence oversight guidelines. In the past, all the concern and oversight has been directed toward intelligence personnel, units, or activities. The following is general regulatory guidance for non-MI personnel:

(1) The PM/J34 carries out the following responsibilities: "Initiate and maintain liaison with Federal, State, Tribal and local law enforcement agencies; gather and report information on domestic activities that pose a threat to NG resources, facilities, and activities" in accordance with DoD O-2000.12-H DoD Antiterrorism Handbook (ref 1h). The PM / J34 consists of non-intelligence entities within the Office of the Provost Marshal and J34 that are not subject to the provisions of AR 381-10, US Army Intelligence Activity (ref 1m) & AFI 14-104, Oversight of Intelligence Activities (ref 1i), but complies with DoDD 5200.27 which allows DoD components to gather information essential to the protection of DoD functions and property.

(2) Non-MI personnel cannot collect, report, process, or store info concerning activities of individuals or organizations not affiliated with DoD, except under the following mission essential elements:

(a) for the Protection of DoD Functions and Property

(b) for Personnel Security

(c) and for Operations Related to Civil Disturbances in Title 10/32 w/SECDEF approval.

(3) Retained information regarding USPERS shall be destroyed within 90 days unless otherwise authorized.

(4) Authorized information stored is subject to annual review and verification to determine threat is still valid (ref 1b).

(5) No computer data bases may be maintained.

b. JFHQ-State PMs/J34s are governed by the provisions of reference 1b. They are responsible for tracking and analyzing criminal threats to DoD and domestic threats to DOD. PM/J34 personnel liaise with other Law Enforcement Agencies (LEAs) and develop the Criminal Threat Situational Picture.

c. JFHQ-State Civil Support Teams (CST), Critical Infrastructure Protection – Mission Assurance Assessments (CIP-MAA) and the CBRNE-Enhanced Response Force Package (CERFP) units are governed by the provisions of DoDD 5200.27.

8. Proper handling of USPERS information.

a. Intelligence Oversight applies only to USPERS information as defined by governing regulations and as listed above. It is the responsibility of JFHQ-State J2s to be fully cognizant of how this affects retention of intelligence and information files related to their assigned duties. NG Intelligence personnel may receive information from anyone, at anytime to further evaluate to see if the information contains a foreign nexus and supports their authorized mission, or if it must be forwarded to the appropriate civilian or military law enforcement or DoD Anti-Terrorism /Force Protection section. You may use USPERS info when it is necessary to an authorized function and the info falls within one of 13 categories specified in DoD 5240.1-R, Procedure 2 such as: Information obtained with consent, Publicly available information, Foreign Intelligence, Counterintelligence, International Narcotics Activities.

b. DoDD 5200.27 and AR 380-13, Acquisition of Information Concerning Persons and Organizations Not-Affiliated with the Department of Defense, applies to other non-Military Intelligence (MI) staff elements. States need to coordinate with their JA and Inspector General (IG) to ensure proper awareness training is conducted, and activities of non-MI functions are conducted IAW published directives and regulations.

c. National Guard Counterdrug Program: The NG does not conduct Intelligence activities of its own in Counterdrug Support Program missions. National Guard members support the criminal information analysis activities of LEAs. Criminal information comes into temporary possession of National Guard members supporting

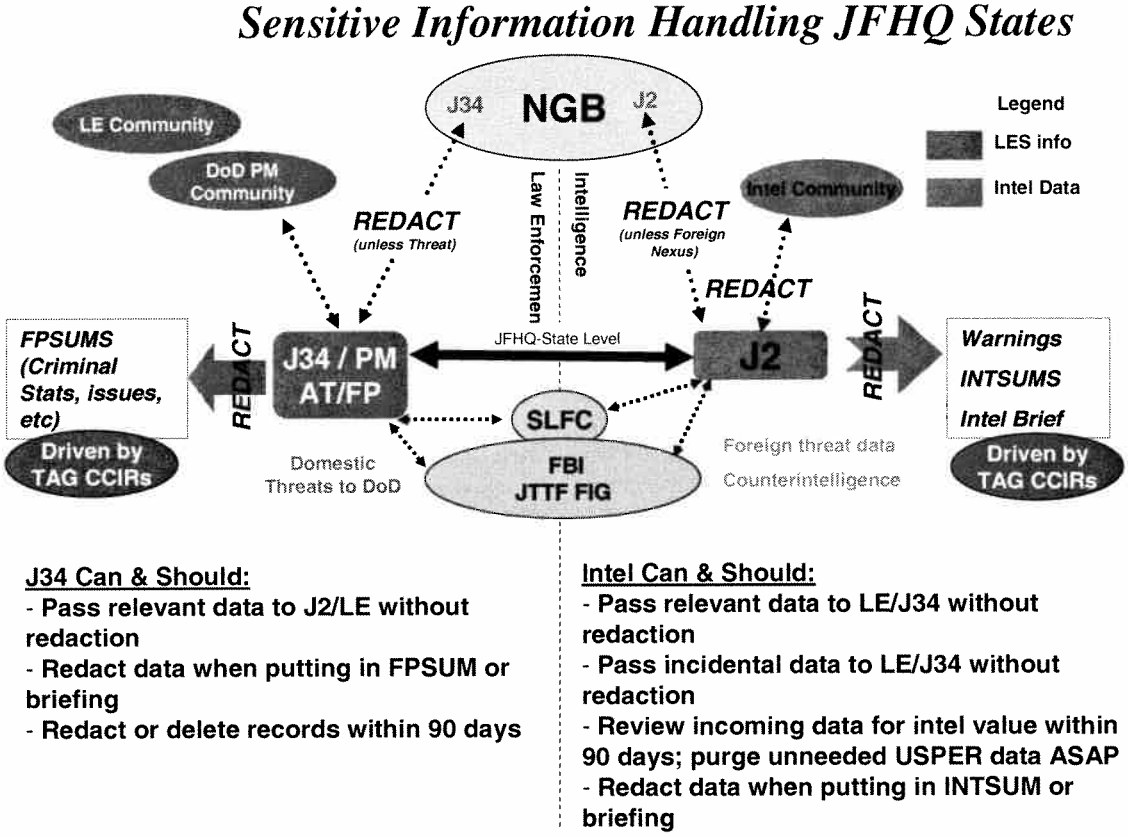
LEAs but is not retained by the National Guard. Counterdrug Coordinators coordinate with LEAs to ensure support of intelligence LEA operations is conducted in accordance with applicable directives and in the support role intended by Counterdrug Support Program policy. This requires periodic monitoring of the daily routines and actual duties performed by National Guard members.

9. Proper use of Military Intelligence Equipment. Military Intelligence Equipment may only be used to conduct foreign intelligence related missions unless separate authorizations have been granted IAW ref 1k. Therefore, this equipment may only be operated by NG intelligence personnel serving in a Title 10 or Title 32 status. States wishing to utilize this equipment for other than foreign intelligence purpose must request authorization from the NGB-J2. Legal review by NGB-JA is required prior to such authorizations. Some Military Intelligence Equipment are, but not limited to SIPRnet, JWICS, and ASAS-L (All Source Analysis System-Light).

10. Sharing of Intelligence Information:

a. Intelligence components have an obligation to pass threat information to the organization commander and/or agencies responsible for protecting the threatened persons and/or assets. Intelligence personnel have 90 days to evaluate the information, but do not have to retain it for the entire 90 days and should pass it upon determination. The fact that USPERS information is routinely part of Federal, State, Local and Tribal homeland security efforts does not in any way preclude effective liaising and coordination between JFHQ-State J2s and their intelligence partners in support to Force Protection and the TAG's Commanders Critical Information Requirements (CCIRs). These partners include the FBI - Field Intelligence Group (FIG), the Department of Homeland Security state intelligence liaison to the State Fusion Centers, State Emergency Management and State Homeland Security Departments, and other members of the intelligence community.

b. Information Sharing Process. The chart below illustrates how the flow of information occurs to be compliant with intelligence oversight regulations. It graphically shows how the J2 and PM/J34 share and handle sensitive information (e.g. USPERS) IAW both Intelligence Oversight regulations and DoDD 5200.27.



c. The FBI is the lead federal agency for CONUS threat intelligence; coordination should be conducted with them to verify a foreign nexus and threat to DoD assets or personnel as soon as possible. If a foreign nexus cannot be verified, the USPERS data will be passed to the appropriate LE agency or DoD Anti-Terrorism / Force Protection section without minimization or redaction of USPERS information and intelligence files will be purged of the information.

d. Intelligence personnel have 90 days to evaluate the information, but generally it can be determined in a relatively short time. Intelligence personnel should practice "Minimization" and thereby only retain the minimal amount of USPERS info necessary for mission accomplishment while eliminating un-needed personal information (redaction) from documents intended for Joint Task Force consumption.

e. If the status (LE or foreign) of the USPERS information can't be immediately determined and the information is retained, then the 90 day period begins. If in electronic form, a "hard-copy" will be produced and the electronic form will be deleted from intelligence computers and files. This "hard-copy" will be marked at the top and

bottom of the document that contains the USPERS information with a statement and date: "USPERS information - Destroy NLT DATE" of end of 90 day period). A cover sheet will be made and attached indicating reason for retaining the information, authority to retain the information, and the NLT destruction date. This will be maintained in a separate file and routinely check and direct effort made to determine the retention status so the information can either be destroyed or passed to the appropriate LEA. No computerized data banks shall be maintained containing information on civil disturbances or on persons and organizations not affiliated with the Department or Defense unless authorize by NGB-J2.

11. NGB-J2 continues to work with JFHQ-State J2 functions through the J2 Functional Area Council to develop more effective resources and training tools to assist you in your IO program implementation.

12. The JFHQ-State J2 is the proponent for the State IO program, to include training guidance and coordination with IG and JA representatives. NG intelligence personnel within the state should direct IO questions to the JFHQ-State J2, their State IO manager, or IG and JA representatives. State IO programs should clearly define the procedures for individuals seeking additional IO guidance.

13. Training.

a. Intelligence Oversight: There are several knowledge resources available on the web that can be used to assist in establishing, maintaining, or bolstering effective IO programs for JFHQ-State J2 functions and other personnel requiring training due to their handling of US person information.

(1) The NGB-J2 GKO web portal https://gko.ngb.army.mil/Login/welcome.aspx

(2) The NGB J2 Community of Practice https://afkm.wpafb.af.mil/ASPs/CoP/EntryCoP.asp?Filter=OO-SF-AN-50

(3) The NGB-IG GKO web portal https://gko.ngb.army.mil/Login/welcome.aspx

(4) Assistant to the Secretary of Defense for Intelligence Oversight NIPRnet: www.dod.mil/atsdio and SIPRnet: www.atsdio.ismc.sgov/atsdio.

(5) The ATSD IO the Air Force's 33rd Wing at Eglin Air Force Base at http://www.defenselink.mil/atsdio/briefing/io_briefing_1.html

(6) The Air Force Portal Intelligence Oversight Community of Practice https://afkm.wpafb.af.mil/ASPs/CoP/OpenCoP.asp?Filter=OO-IN-AF-15

b. The illustration in paragraph 10 is also helpful in understanding flow and the process of handling information.

c. JFHQ-State J2 and PM/J34 may seek additional clarification on specific IO issues by contacting NGB-J2 if neither their state IG nor JA, nor existing references / websites offer a clear solution.

13. This memorandum will expire one year from date of publication unless sooner rescinded or superseded.

14. The POCs for this Policy Memorandum are Deputy Director, NGB-J2 at 703-607-1822 and the Provost Marshal, NGB-PM/J34 at 703-607-8718.

H STEVEN BLUM
Lieutenant General, USA
Chief, National Guard Bureau