CHIEF OF THE NATIONAL GUARD BUREAU INSTRUCTION

NGB-J3/4/7 CNGBI 3000.07
DISTRIBUTION: A 15 November 2023

ACQUISITION AND STORAGE OF INFORMATION CONCERNING PERSONS AND ORGANIZATIONS NOT AFFILIATED WITH THE DEPARTMENT OF DEFENSE

References: See Enclosure B.

1. Purpose. This instruction establishes policy and assigns responsibilities for acquiring, processing, retaining, and disseminating information concerning persons or organizations not affiliated with the Department of Defense (DoD) in accordance with (IAW) references a, b, c, and d.

2. Cancellation. This instruction cancels and replaces CNGBI 2400.00A, 07 November 2013, "Acquisition and Storage of Information Concerning Persons and Organizations Not Affiliated With The Department of Defense," Validity extended to 01 March 2021.

3. Applicability. This instruction applies to Service members assigned to National Guard Bureau (NGB) and all National Guard (NG) personnel serving in a Title 32 (T32) duty status, NG Title 5 Technicians, T32 NG Joint Force Headquarters-State (NG JFHQs-State), and T32 NG non-intelligence units and staff organizations, hereinafter referred to as the NG. NG members serving in a Title 10 (T10) status with the Active Components will comply with Service-specific regulations. This instruction does not apply to the NG intelligence component, as defined in the glossary, which are subject to Intelligence Oversight rules IAW references e, f, g, h, and i. This instruction does not apply to NG personnel while in a State Active Duty (SAD) status, State employees, or suspicious activity reporting by individual NG members. This instruction does not exclude acquisition of information that is required by Federal statute or Executive order.

4. Policy. It is NGB policy that the NG is prohibited from acquiring, reporting, processing, and storing information on persons and organizations not affiliated with the DoD, except in those limited circumstances where such information is essential to accomplishing an authorized mission. Information-gathering activities will be subject to overall civilian control, high levels of general supervision, and frequent inspections.

a. General. All authorized NG information acquisition activities must protect the Constitutional and privacy rights and civil liberties of U.S. persons and comply with Federal law, DoD regulations, and Service-specific guidance IAW reference b and reference c.

(1) Only NG Provost Marshals (PM) and PM staffs, Security Forces (SF) and Security Forces staffs, Military Law Enforcement Officers, and Antiterrorism Officer personnel associated with law enforcement elements may acquire information on non-DoD non-NG affiliated civilians IAW references g, j, k, l, m, and n for the purpose of protecting DoD and NG personnel, functions, and property. Consistent with applicable law, information about an individual or organization that is acquired will be legally authorized, relevant, and necessary to accomplish an established DoD or NG mission or function. In addition, information contained in a Privacy Act system of records will be maintained consistent with the requirements set forth under reference b and the relevant System of Records Notice(s). Information indicating that alleged activities or crimes are conducted for or on behalf of foreign powers, organizations, persons, or their agents, or international terrorist organizations will be reported to Counterintelligence agencies IAW references e, f, g, h, and i.

(2) NG Counter Drug (CD) element personnel supporting civilian Law Enforcement Agencies (LEA) must comply with procedures in references o, p, and q. Law Enforcement criminal analysis information is the property of the supported LEA and is not intelligence information. NG criminal analysts will return the raw information and provide resultant analysis to the civilian LEA and will not retain the data in any Federal NG file or database IAW references o, p, and q.

(3) NG Chemical Biological Radiological and high yield Explosive Response Enterprise Weapons of Mass Destruction-Civil Support Teams, Homeland Response Forces, and Chemical Biological Radiological and high yield Explosive Response Enhanced Response Force Commanders will ensure that any information concerning any non-DoD affiliated person or organization gathered during operations IAW references r and s will not be disseminated or retained upon operation completion. All entries regarding non-DoD persons and organizations information in the Civil Support Team Incident Management System unit logs and Mobile Field Kit (SQL) database will be redacted from the system upon mission completion.

(4) NG regulations, instructions, and policy governing PM activities, NG Chemical Biological Radiological and high yield Explosive Response Enterprise, CD non-intelligence activity and antiterrorism and force protection activities will include specific guidance on the acquisition, retention, and dissemination of information concerning organizations and persons not affiliated with the DoD.

b. Authorized Missions. Authorized missions IAW references b and c where the NG may acquire information regarding persons or organizations not affiliated with DoD that is essential to mission accomplishment are:

(1) Protection of DoD and NG Functions and Property. NG functions, and property are those that are funded by DoD through the State (for example, through a Master Cooperative Agreement), or are necessary to the accomplishment of Federally funded NG missions (for example, a State-owned armory). Information may be acquired about individuals, organizations, or activities posing a threat to DoD and NG military or civilian employees, activities, equipment, and supplies. Only the following

types of activities identified in reference c justifies acquisition of information for protection of DoD and NG functions and property:

(a) Subversion of loyalty, discipline, or morale of DoD and NG military or civilian personnel by actively encouraging violation of law, disobedience of lawful order, regulation or instruction, or disruption of military activities.

(b) Theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD and NG units or installations.

(c) Acts jeopardizing the security of DoD and NG elements or operations or compromising classified defense information by unauthorized disclosure.

(d) Unauthorized demonstrations on Active or Reserve DoD and NG installations.

(e) Direct threats to DoD and NG military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD and NG resources.

(f) Activities endangering facilities that have classified defense contracts or that have been officially designated as key defense facilities.

(g) Crimes for which the DoD and NG have responsibility for investigating or prosecuting.

(2) Personnel Security. The NG may request that investigations be conducted by the appropriate DoD agency in relation to the following categories of persons. (Refer to unit, organization, or staff security manager for specific guidance.)

(a) Members of the Armed Forces, including retired personnel, members of the Reserve components, and applicants for commission or enlistment.

(b) DoD and NG civilian personnel and applicants for such status.

(c) Persons having the need for access to official information requiring protection in the interest of national defense under the DoD and NG Industrial Security Program or being considered for participation in other DoD and NG programs.

(3) Operations Related to Civil Disturbance. State and Territorial Governors, and local governments are responsible for maintaining Law and Order within their respective jurisdictions. NG personnel will usually respond to civil disturbances in SAD status under control of their respective State Governor and The Adjutant General (TAG). If a Civil Disturbance exceeds the capabilities of State and local authorities, Federal assistance may be requested or required to restore law and order. The Department of Justice is the primary Federal agency for coordinating Federal

Government response to restore law and order. The U.S. Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. In the event of a Federal civil disturbance response, NG personnel and units may be Federalized to a T10 status as part of DoD activities to support the U.S. Attorney General's response efforts.

(a) SAD. NG forces responding to a civil disturbance in SAD status are governed by the State, Territorial, or local laws where the operation occurs. Any information concerning persons or organizations not affiliated with DoD acquired, retained, or disseminated by non-Federalized NG personnel in SAD supporting a State mission must be essential to meet the operational requirements of the mission assigned to TAG by the Governor. Federal records needed to execute SAD missions cannot be transferred to the State government without prior approval from the originator of the document and released IAW guidelines in reference t.

(b) T32. NG forces responding to civil disturbances while in a T32 status remain under the command and control of the Governor and TAG and are governed by State law regarding military justice. The acquisition, use, maintenance, or dissemination of information related to individuals not affiliated with the DoD, however, is governed by references b, c, and the regulation of the non-federalized National Guard under Titles 10 and 32 of the U.S. Code.

(c) T10. Upon T10 mobilization, Federalized NG personnel must follow Service-specific and DoD policies in executing Service missions.

c. Prohibited Activities. IAW reference b and reference c, the NG will not:

(1) Acquire information about a person or an organization solely because of lawful advocacy of measures in opposition to U.S. Government policy.

(2) Conduct physical or electronic surveillance of Federal, State, or local officials or candidates for such offices.

(3) Conduct electronic surveillance of any individual or organization, except as authorized by law.

(4) Conduct, or otherwise use, covert or deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense or designee.

(5) Assign personnel to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the acquisition of which is authorized by this instruction, without specific prior approval from the Secretary of Defense, or his or her designee. An exception to this policy may be made by the local commander or higher authority when, in his or her 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 Secretary of Defense, or his or her designee, through the NGB PM.

(6) Maintain computerized databases relating to individuals or organizations not affiliated with the DoD, unless one of the following applies:

(a) A System of Records Notices is published in the Federal Register allowing for the acquisition of information on individuals.

(b) The Secretary of Defense has authorized acquisition of information on persons and organizations.

d. Training Requirements. Training will be monitored by Commanders or Directors through an appointed Program Monitor who will maintain a non-DoD persons information protection continuity binder. The binder may be in electronic or hard copy format and will contain items listed in Table 1 below.

✓ Appointment letters for primary and alternate Program Monitors. ✓ Program Monitor duties and responsibilities. ✓ Unit non-DoD persons information protection training. ✓ Program training records (initial and annual). ✓ Copies of references a, c, and this instruction. ✓ Joint and Army National Guard (ARNG) programs must also have a copy of reference m. ✓ Unit-oriented program self-inspection checklist. ✓ Self-inspection and inspection records. ✓ Annual file review certification memorandum for record.

Table 1. Continuity Binder Contents

(1) Personnel assigned to NGB, T32, NG JFHQs-State, and T32 NG non-intelligence units and staff organizations that can acquire, retain, and disseminate information concerning persons and organizations not affiliated with the DoD must receive training within 90 days of assignment or employment followed by annual refresher training that complies with Service Component regulations.

(2) NG CD personnel not involved in military intelligence support that can acquire, retain, and disseminate information concerning persons and organizations not affiliated with the DoD must receive training at initial entry and annually thereafter. NG CD personnel involved in intelligence support are not subject to this instruction and will comply with Intelligence Oversight training requirements, IAW references e, f, g, h, and i.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. There are substantive changes to this instruction include the transfer of responsibility for this NGB policy from the Joint Intelligence Directorate (NGB-J2) to the Operations Directorate (NGB-J3/4/7), issuance renumbering, and definition of the role of NG PM.

8. Releasability. This instruction is approved for public release; distribution is unlimited. It is available at <https://www.ngbpmc.ng.mil/>.

9. Effective Date. This instruction is effective upon publication and must be reviewed annually by the Proponent/Office of Primary Responsibility for continued validity, and revised, reissued, canceled, or certified as current every ten years.

DANIEL R. HOKANSON
General, USA
Chief, National Guard Bureau

Enclosures:

A -- Responsibilities
B -- References
GL -- Glossary

ENCLOSURE A

RESPONSIBILITIES

1. Director of the Army National Guard and Director of the Air National Guard. The Director of the Army National Guard and Director of Air National Guard will implement this policy for acquiring, processing, retaining, and disseminating information concerning persons or organizations not affiliated with DoD within the Army National Guard and Air National Guard of the States, Territories, and the District of Columbia.

2. Office of the NGB Inspector General Intelligence Oversight Division. The Office of the NGB Inspector General Intelligence Oversight Division will comply with duties as specified in reference u.

3. Office of the NGB General Counsel. The Office of the NGB General Counsel will:

a. Be familiar with missions, plans, and capabilities of NG organizations, units, and staffs tasked to acquire, process, retain, and disseminate information concerning non-DoD affiliated persons and organizations, and applicable laws, Executive orders, regulations, instructions, and other policies that apply to their activities, including the restrictions on such acquisition, retention, and dissemination.

b. Ensure Office of the NGB General Counsel personnel receive training as described in this instruction.

c. Provide legal counsel for matters concerning acquisition, processing, retention and dissemination of information by the NG regarding persons or organizations not affiliated with the DoD.

d. In coordination with State Judge Advocates, provide interpretation of applicable Federal laws; Executive orders; directives; regulations and instructions that relate to the NG acquiring, processing, retaining, and disseminating information regarding persons or organizations not affiliated with the DoD.

e. Review legality and propriety of any NG plans, proposals, and concepts that include acquiring, processing, retaining, and disseminating information regarding persons or organizations not affiliated with DoD.

f. Assist with training NG staff members regarding Executive orders, laws, policies, treaties, and agreements pertinent to acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with the DoD.

4. Director of NGB-J3/4/7. The Director of NGB-J3/4/7 will:

a. Serve as the Office of Primary Responsibility for this instruction.

b. Be familiar with missions, plans, and capabilities of NG organizations, units, and staffs that are tasked to acquire, process, retain, and disseminate information concerning persons or organizations not affiliated with DoD.

c. Ensure specific guidance on the acquisition, retention, and dissemination of information concerning non-DoD persons and organizations is included in regulations, instructions and other policy governing organizations, units, and staffs that are tasked to conduct these activities.

5. TAGs and the Commanding General of the District of Columbia. TAGs and the Commanding General of the District of Columbia, under the authority, direction, and control of their Governors or chain of command, will:

a. Be familiar with all NG organizations, units, or staffs in a T32 status that acquire, process, retain, and disseminate information concerning persons or organizations not affiliated with DoD.

b. Develop and publish policy and procedures for the respective State or territory to ensure acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD are conducted IAW this instruction.

c. Ensure compliance with this instruction.

6. NG JFHQs-State Inspectors General. NG JFHQs-State Inspectors General should perform duties as specified in reference u for organizations or units within their respective State that acquire, process, retain, and disseminate non-DoD persons information will:

a. Know what organizations, units, or staffs under NG JFHQs-State Inspector General's jurisdiction, acquire, process, retain, and disseminate non-DoD persons information and organizations.

b. Ensure Inspector General personnel are trained IAW this instruction.

7. NG JFHQs-State Judge Advocates and other Legal Advisors. NG JFHQs-State Judge Advocates and other legal advisors will:

a. Know what organizations, units, and staffs, under State Judge Advocate jurisdiction, acquire, process, retain, and disseminate information about persons or organizations not affiliated with DoD.

b. Advise Commanders, Directors, or personnel on all matters regarding acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

c. Be familiar with missions, plans, and capabilities of NG organizations,

units, or staffs in the State that are tasked to acquire, process, retain, and disseminate information concerning persons or organizations not affiliated with DoD.

d. Ensure State Judge Advocate personnel receive training.

e. Advise TAGs and the Commanding General of the District of Columbia, and State NG entities concerned regarding acquiring, processing, and disseminating information about persons or organizations not affiliated with DoD.

f. Interpret applicable Federal, tribal, and State laws, Executive orders, directives, regulations, and instructions related to the to the NG acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

g. Review all State NG plans, proposals, and concepts that include acquiring processing, retaining, and disseminating non-DoD persons information for legality and propriety, as required.

h. Assist with training NG JFHQs-State staff members regarding Executive orders, laws, policies, treaties, and agreements pertinent to acquiring, processing, and disseminating information about persons or organizations not affiliated with DoD.

8. NG JFHQs-State PM, and NG JFHQs-State J-34 Staffs. NG JFHQs-State PMs, NG JFHQs- State J-34 staffs will:

a. Provide NG leadership with information and recommendations to assist decision making pertaining to antiterrorism and force protection, critical infrastructure, security, and law enforcement activities. NGB and NG JFHQs-State NG PMs, and J-34 personnel track and analyze criminal and domestic threats to the NG, coordinate with other Federal, State, and local LEAs, and develop the criminal threat situational picture. This is accomplished through review, analysis, and distribution of law enforcement threat information.

b. Ensure all information concerning non-DoD persons and organizations indicate a significant and relevant threat to the NG mission (current or future), personnel, and infrastructure.

9. Commanders and Directors of Non-intelligence Organizations. The Commanders and Directors, or equivalent, of non-intelligence organizations will:

a. Be familiar with the missions, plans, and capabilities of subordinate units that acquire, process, retain, and disseminate information about persons or organizations not affiliated with DoD, and assign tasks and missions IAW applicable policy guidance.

b. Receive training.

c. Establish and maintain a program for protecting information about persons

or organizations not affiliated with DoD for all personnel assigned or attached to the organization, unit, or staff.

d. Be responsible to their respective TAG for oversight of the program to protect information about persons not affiliated with DoD.

e. Appoint primary and alternate Program Monitors in writing to perform the functions listed in paragraph b. below.

f. Ensure compliance with this instruction and ensure appropriate sanctions are imposed upon any employee who violates its provisions.

10. Program Monitors. Program Monitors will:

a. Implement a non-DoD persons information protection program to educate and train all personnel who acquire, process, retain, and disseminate non-DoD persons information on applicable policy.

b. Conduct training for personnel who acquire, process, retain, and disseminate information about persons or organizations not affiliated with DoD IAW this instruction within 90 days of assignment and annually thereafter. Additionally, Program Monitors will maintain records of this training IAW the published Records Disposition Schedule.

c. Maintain a continuity book for the information protection program.

d. Ensure copies of reference c, this instruction, and State policies are maintained and available to the organization in hard copy or electronic form. Joint and Army National Guard organizations, units, and staffs must also maintain a copy of reference v.

e. Perform a self-inspection in the final quarter of the calendar year if NGB Office of the Inspector General Intelligence Oversight Division has not evaluated the program in the current calendar year.

f. Provide advice regarding retaining information on persons and organizations not affiliated with DoD.

g. Review all documents, electronic and paper, at a minimum, once a calendar year to ensure all non-DoD persons information retained is IAW this instruction and certify that all files have been reviewed through a memorandum for record, which will be maintained on file in the program continuity book.

11. Personnel Authorized to Acquire, Process, Retain, and Disseminate Non-DoD Persons Information. Personnel who are authorized to acquire, process, retain, and disseminate non-DoD persons information will:

a. Know the authorized mission of the organization, unit, and or staff.

b. Be familiar with this instruction and DoD Service-specific regulations, instructions, or standard operating procedures concerning acquiring, processing, retaining, and disseminating non-DoD persons information, including requirements for compliance IAW references a, b, c, and d.

c. Complete non-DoD persons information protection training upon assignment or employment. Complete an annual refresher training, and specialized Privacy Act training to be established, in coordination with the local Privacy Officer, by the office responsible for the acquisition of the personal identifiable information IAW reference c and reference d.

d. Report violations of policy and regulations pertaining to the acquisition, processing, retention, and dissemination of Non-DoD persons to the Program Monitor.

ENCLOSURE B

REFERENCES

PART I. REQUIRED

a. Department of Defense (DoD) Directive 5105.77, 30 October 2015, "National Guard Bureau (NGB)," Incorporating Change 1, 10 October 2017

b. Title 5 United States Code, Section 552a, "Privacy Act of 1974"

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

d. DoD 5400.11, 29 June 2019, "DoD Privacy Program"

e. Executive Order 12333, 04 December 1981, "United States Intelligence Activities," (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))

f. DoD 5240.1-R, December 1982, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons"

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

h. Chief of the National Guard Bureau (CNGB) Instruction 2000.01D, 18 January 2022, "The Conduct and Oversight of National Guard Intelligence Activities," Incorporating Change 1, 15 June 2023

i. CNGB Manual 2000.01B, 24 August 2022, "National Guard Intelligence Activities"

j. DoD Instruction 2000.26, 04 December 2019, "DoD Use of the Federal Bureau of Investigation (FBI) e-Guardian System"

k. DoD Instruction 5505.17, 17 October 2013, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," Incorporating Change 3, 03 August 2020

l. DoD Instruction 5525.18, 18 October 2013, "Law Enforcement Criminal Intelligence (CRIMINT) in DoD," Incorporating Change 3, 01 October 2020

m. DoD System of Records Notices listing, <https://dpcld.defense.gov/Privacy/SORNsindex/>, accessed 15 November 2023

n. CNGB Instruction 7102.01, 09 February 2018, "National Guard Provost Marshal's Responsibilities and Selection Criteria"

o. CNGB Instruction 3100.01B, 06 March 2020, “National Guard Counterdrug Support Program”

p. CNGB Manual 3100.01, 30 July 2021, “National Guard Counterdrug Support”

q. Office the Assistant Secretary of Defense for Special Operations and Low Intensity/ Conflict – Memorandum, 07 March 2022, “National Guard Counter Drug Program (CDP) Guidance”

r. CNGB Instruction 3501.00A, 29 April 2022, “Weapons of Mass Destruction Civil Support Team Management’

s. CNGB Manual 3501.00, 10 January 2020, “Weapons of Mass Destruction—Civil Support Team Management (For Official Use Only)”

t. DoD Instruction 5200.48, 06 March 2020, “Controlled Unclassified Information (CUI)”

u. CNGB Instruction 0700.01A, 21 December 2018, “Inspector General Intelligence Oversight”

v. Army Regulation 380-13, 30 September 1974, “Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations”

PART II. RELATED

w. Army Regulation 381-12, 01 June 2016, “Threat Awareness and Reporting Program”

x. Air Force Instruction 33-332, 10 March 2020, “Air Force Privacy And Civil Liberties Program,” Corrective Actions applied on 12 May 2020

GLOSSARY

PART I. ACRONYMS

ARNG	Army National Guard
CST	Civil Support Team
DoD	Department of Defense
IAW	In accordance with
LEA	Law Enforcement Agency
NG	National Guard
NG JFHQs-State	National Guard Joint Force Headquarters-State
NGB	National Guard Bureau
NGB-J2	Joint Intelligence Directorate
NGB-J3/4/7	Operations Directorate
NGB-J34	Logistics, Engineering, and Protection Division
PM	Provost Marshal
SAD	State Active Duty
TAG	The Adjutant General
T10	Title 10 United States Code
T32	Title 32 United States Code
WMD-CST	Weapons of Mass Destruction Civil Support Team

PART II. DEFINITIONS

Affiliation with the Department of Defense -- An individual, group of individuals, or organization is considered to be affiliated with Department of Defense if the persons involved are one of the following:

a. Employed by or contracting with the Department of Defense or any activity under the jurisdiction of Department of Defense, whether on a full-time, part-time, or consultative basis.

b. Members of the Armed Forces on active duty, National Guard members, those in a reserve status, or in a retired status.

c. Residing on, having authorized official access to, or conducting or operating any business or other function at any Department of Defense installation or facility.

d. Having authorized access to defense information; or participating in other authorized Department of Defense programs.

e. Applying for or being considered for any status described in a through d above, including individuals such as applicants for military service, pre-inductees and prospective contractors.

Intelligence Activity -- All activities that Department of Defense intelligence components are authorized to undertake pursuant to reference f. Note that reference f assigns the Services' intelligence components' responsibility for:

a. The collection, production, and dissemination of military and military related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking.

b. Monitoring the development, procurement, and management of tactical intelligence systems. This includes intelligence activities conducted by non-intelligence organizations.

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 weapons system that their primary function is to provide immediate use targeting data.)

NG Intelligence Component -- 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 rules without exception. NG intelligence personnel operating in a State Active Duty status are not members of the Department of Defense intelligence component and are prohibited from engaging in a Department of Defense intelligence or counterintelligence mission or using intelligence or counterintelligence systems, resources, or equipment, and, therefore, not subject to Federal intelligence oversight policies. In State Active Duty status, they are subject to State laws, including State privacy laws. In most States, the collection, use, maintenance, and dissemination of personal information is strictly regulated; therefore, NG members in a State Active Duty status should seek competent legal advice on State laws before collecting information on United States persons.

Personally Identifiable Information -- As defined in reference k, personally identifiable information refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of personally identifiable information is not anchored to any single category of information or technology. It requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-personally identifiable information can become personally identifiable information when ever additional information is made publicly available in any medium and from any source that, when combined with other available information, could be used to identify an individual.

System of Records -- This is defined by reference b as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Notice -- The notice(s) published by an agency in the *Federal Register* upon the establishment and/or modification of a system of records describing the existence and character of the system.