CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NG-J2 CNGBI 2400.00A CH 1
DISTRIBUTION: A 07 November 2013

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

References: See Enclosure D.

1. Purpose. This instruction establishes National Guard (NG) policy and responsibilities for acquiring, processing, retaining, and disseminating information concerning persons or organizations not affiliated with the Department of Defense (DoD), and implements guidance in accordance with (IAW) reference a.

2. Cancellation. None.

3. Applicability.

a. This instruction applies to all NG personnel serving in a Title 32 (T-32) status, NG technicians, T-32 NG Joint Force Headquarters-State (JFHQ-S), and T-32 NG non-intelligence units and staff organizations, hereafter referred to as the NG. NG members serving in a Title 10 (T-10) status must comply with Service specific regulations.

b. This policy does not apply to the National Guard Bureau (NGB) and the NG intelligence component, defined as NG intelligence units and staff organizations and non-intelligence organizations that perform intelligence or intelligence-related activity, as defined in the glossary. These personnel and activities are subject to intelligence oversight (IO) rules IAW references b, c, and d. This policy does not apply to NG personnel while in a State Active Duty (SAD) status, or to State employees.

c. This policy does not exclude acquisition of information required by Federal statute or Executive Order (EO).

4. Policy. The NG is prohibited from acquiring, reporting, processing, and storing information on individuals and organizations not affiliated with the DoD, except in those limited circumstances where such information is essential to the accomplishment of an authorized mission. Information-gathering activities will be subject to overall civilian control, high levels of general supervision, and frequent inspections. The NG is authorized to gather information essential to the accomplishment of the following missions:

a. Protection of DoD and NG functions and property. NG functions and property are those that are funded by DoD through the State (e.g., through a Master Cooperative Agreement), or are necessary to the accomplishment of federally funded NG missions (e.g., 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. The acquisition of personally identifiable information (PII) may only be done IAW a published System of Records Notices (SORN). A listing of DoD SORNs can be found in reference e. If found that the investigated, alleged activities or crimes that are conducted for or on behalf of foreign powers, organizations, persons or their agents, or international terrorist organizations, the incident should be handled and investigated by counterintelligence (CI) personnel, and, therefore, turned over to the proper agency, the nearest 902nd Military Intelligence (MI) Field Office or a Federal Bureau of Investigation (FBI) field office IAW references f and g. Only the following types of activities justify acquisition of information for protection of DoD and NG functions and property:

(1) 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.

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

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

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

(5) 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.

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

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

b. Personnel Security. The NG may request that investigations be conducted by the appropriate DoD agency ~~Defense Manpower Data Center~~ in relation to the following categories of persons. Refer to unit, organization or staff security manager for specific guidance.~~:~~

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

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

(3) 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 authorized DoD and NG programs.

c. Operations related to Civil Disturbance.

(1) The Department of Justice (DoJ). The DoJ is the primary Federal agency for coordinating Federal Government response to restore law and order. The Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. Upon specific, prior authorization from the Secretary of Defense (SecDef) or his or her designee, federalized T-10 NG personnel must follow Service-specific policies in executing service missions.

(2) SAD. NG forces responding to a civil disturbance while in SAD status are governed by the laws of the State 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 operational requirements flowing the mission assigned by the Governor through The Adjutant General (TAG). 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 h.

(3) T-32. NG forces responding to civil disturbances while in a T-32 status are under the command and control of the Governor and TAG, and are governed by State law regarding military justice and command and control. However, the acquisition, use, maintenance and dissemination of information related to individuals not affiliated with the DoD is covered in reference i and

the Federal regulations regarding the management of information pursuant to the supremacy clause of the U.S. Constitution.

d. Prohibited Activities. 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 of 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 SecDef, or his or her 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 SecDef, 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 SecDef, or his or her designee, through the NGB.

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

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

(b) The SecDef has authorized acquisition of information on organizations.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. This is the initial publication of CNGBI 2400.00.

8. Releasability. This instruction is approved for public release; distribution is unlimited. NGB directorates, TAGs, the Commanding General of the District of

Columbia, and JFHQ-S may obtain copies of this instruction through <http://www.ngbpdc.ngb.army.mil>.

9. Effective Date. This instruction is effective upon publication and must be reissued, cancelled, or certified as current within five years of its publication.

FRANK J. GRASS
General, USA
Chief, National Guard Bureau

Enclosures:

A -- Responsibilities
B -- Program Continuity Binder
C -- References
GL -- Glossary

ENCLOSURE A

RESPONSIBILITIES

1. Office of the Chief of the National Guard Bureau/NG Joint Staff.

a. Director, NG Domestic Operations (NG-J3). The Director, NG-J3 will:

(1) Assume responsibility for this instruction one year from date of publication, and review this instruction IAW the effective date paragraph above.

(2) 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.

(3) 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. Regulations, instructions and policy governing Civil Support Teams (CST), Counterdrug (CD) non-intelligence activity and Antiterrorism/Force Protection (AT/FP) activities will include specific guidance on the acquisition, retention, and dissemination of information concerning organizations and persons not affiliated with the DoD.

(a) Training on the protection of CD program-related information concerning persons and organizations not affiliated with DoD will be included in doctrinal training given to NG CD personnel not involved in MI support at initial entry and annually thereafter. CD programs specifically requesting MI Support will have formal IO programs and training, and will follow policy and procedures outlined in references b, and c.

(b) NG CD element personnel supporting civilian Law Enforcement Agencies (LEA) must comply with procedures in reference j.

(c) Law Enforcement (LE) criminal analysis information is the property of the supported LEA and is not intelligence information. NG criminal analysts will provide the raw information and resultant analysis to the civilian LEA, and will not retain the data in any Federal NG file or database.

(d) IAW reference k, Weapons of Mass Destruction-Civil Support Team (WMD-CST) Commanders will ensure that any information gathered during operations concerning any non-DoD person or organization will not be disseminated or retained upon completion of operations.

(e) The current version of the Civil Support Team Incident Management System (CIMS) does not allow WMD-CSTs to alter any entries. Therefore WMD-CSTs are currently unable to redact non-DoD persons information that has been entered into CIMS upon mission completion.

b. NGB Office of the Inspector General (IG) Intelligence Oversight Division (NGB-IGO). NGB-IGO will comply with duties as specified in reference l.

c. NGB Office of the Chief Counsel (NGB-JA). NGB-JA will:

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

(2) Ensure NGB-JA personnel receive training as described in Enclosure B.

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

(4) In coordination with State JAs, provide interpretation of applicable Federal laws; EOs; directives; regulations and instructions that relate to the NG acquiring, processing, retaining and disseminating information regarding persons or organizations not affiliated with the DoD.

(5) Review for legality and propriety any NG plans, proposals, and concepts that include acquiring, processing, retaining, and disseminating information regarding persons or organizations not affiliated with the DoD.

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

d. The Army National Guard (ARNG) Assistant Chief of Staff of Operations (ARNG-G3). ARNG-G3 will implement and oversee the policy for acquiring, processing, retaining and disseminating information concerning persons or organizations not affiliated with DoD within the ARNG of the States, Territories, and District of Columbia.

e. The Air National Guard (ANG) Director of Air, Space and Information Operations (NGB/A3). The Director, NGB/A3 is responsible for the

implementation and oversight of policy for acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with the DoD within the ANG of the States, Territories, and District of Columbia.

2. JFHQ-S.

a. TAGs. TAGs will:

(1) Be familiar with all NG organizations, units or staffs in a Title 32 status that acquire, process, retain, and disseminate information concerning persons or organizations not affiliated with DoD.

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

(3) Ensure compliance with this instruction.

(4) Levy tasks and missions IAW this instruction.

b. JFHQ-S IG. JFHQ-S IGs will perform duties as specified in reference l. Additionally, JFHQ-S IGs responsible for organizations or units that acquire, process, retain, and disseminate non-DoD persons information will:

(1) Know what organizations, unit, or staffs under JFHQ-S IGs jurisdiction, acquire, process, retain, and disseminate non-DoD persons information.

(2) Ensure IG personnel are trained IAW Enclosure B.

c. JFHQ-S Judge Advocates (JA) and other legal advisors. JFHQ-S JAs, JFHQ-S JAs and other legal advisors will:

(1) Know what organizations, units, and staffs, under JA jurisdiction, acquire, process, retain, and disseminate information about persons or organizations not affiliated with DoD.

(2) Advise commanders, directors or personnel on all issues regarding acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

(3) Be familiar with missions, plans, and capabilities of NG organizations, units or staffs in the State that is tasked to acquire, process, retain, and disseminate information concerning persons or organizations not affiliated with DoD.

(4) Ensure State JA personnel receive training as described in Enclosure B.

(5) Advise TAG and State NG entities regarding acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

(6) Interpret applicable Federal, tribal, and State laws; EOs; directives; regulations; and instructions related to the NG acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

(7) 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.

(8) Assist with training JFHQ-S staff members regarding EOs, laws, policies, treaties, and agreements pertinent to acquiring, processing, retaining, and disseminating information about persons or organizations not affiliated with DoD.

d. JFHQ-S Provost Marshal (PM), NG and JFHQ-S J-34 Staffs. JFHQ-S PM, NG and JFHQs J-34 staffs will:

(1) Provide NG leadership with information and recommendations to assist decision-making pertaining to AT/FP, Critical Infrastructure security and LE activities. NG and JFHQ-S PMJ-34 personnel track and analyze criminal and domestic threats to the NG, liaise with other LEAs, and develop the Criminal Threat Situational Picture. This is accomplished through review, analysis and distribution of LE threat information.

(2) 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.

3. Non-Intelligence Organizations, Units and Staffs that Acquire, Process, Retain or Disseminate Information about Persons or Organizations not affiliated with DoD.

a. Commanders and Directors. Commanders and Directors will:

(1) 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 levy tasks and missions IAW applicable policy guidance.

(2) Receive training as described in Enclosure B.

(3) 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.

(4) Be responsible to TAG for oversight of the program to protect information about persons or organizations not affiliated with DoD.

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

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

b. Program Monitors. Program Monitors will:

(1) 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.

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

(3) Maintain a continuity book for the information protection program IAW Enclosure C.

(4) Ensure copies of reference a, this instruction and State policies are maintained and available to the organization in hard copy or electronic form. Joint and ARNG organizations, units and staffs must also maintain a copy of reference m.

(5) Perform a self-inspection in the final quarter of the calendar year if NGB-IGO has not evaluated the program in the current calendar year.

(6) Provide advice regarding retaining information on persons and organizations not affiliated with DoD.

(7) Review all files, 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 (MFR), which will be maintained on file in the program continuity book.

c. Personnel who acquire, process, retain, and disseminate non-DoD persons information. Personnel will:

(1) Know the authorized mission of the organization, unit, and or staff.

(2) Be familiar with this instruction and any Service specific regulation, instruction, or standard operating procedures (SOP) concerning acquiring, processing, retaining, and disseminating non-DoD persons information, to include requirements for compliance IAW references i and n.

(3) Complete non-DoD persons information protection training within 90 days of 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 PII IAW references i and n.

(4) Be able to identify and establish contact with the organization's non-DoD persons protection Program Monitor.

ENCLOSURE B

TRAINING REQUIREMENTS FOR THE PROTECTION OF INFORMATION ABOUT PERSONS AND ORGANIZATIONS NOT AFFILIATED WITH DOD

1. Training Requirements.

a. NGB, T-32 NG JFHQ-S, and T-32 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.

b. Initial training will be conducted within 90 days of assignment or employment followed by annual refresher training.

2. Training development.

a. Personnel will be familiar with this instruction.

b. Training will be tailored to the unit mission and will cover, at a minimum, the following:

(1) Purpose. The purpose of the training is to understand NG policy, limitations, procedures and operational guidance pertaining to acquiring, processing, storing, and disseminating information concerning persons and organizations not affiliated with the DoD. All NG information acquisition activities must protect the Constitutional and privacy rights and civil liberties of U.S. persons while complying with Federal laws, statues, and DoD and Service specific issued guidance.

(2) Status and Applicability.

(a) Intelligence Component. In a T-10 and T-32 status, the intelligence component, those assigned to intelligence or intelligence-related unit, or those conducting intelligence or intelligence-related activity, is not subject to this instruction, but rather must acquire, retain, and disseminate information concerning U.S. persons IAW reference b.

(b) Non-Intelligence Component. In a T-32 status, the non-intelligence component, is subject to the policy set forth in this instruction IAW reference a. NG non-intelligence component members serving in a T-10 status must comply with Service Component regulations.

(c) SAD status. NG personnel in a SAD status are subject to their State laws and not bound to this instruction.

(3) References. Personnel must be familiar with reference a and this instruction.

(4) Scope. This program governs the acquisition, processing, retention, and dissemination of the following:

(a) Persons and organizations not affiliated with the DoD, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. Territories and possessions.

(b) Non-DoD-affiliated U.S. citizens anywhere in the world.

(5) Policy. Personnel must be familiar with all policy in the policy section of this document.

(6) Characteristics of an effective program.

(a) Command and leader emphasis.

(b) Active part of all operational planning and execution, to include the Organization Inspection Program.

(c) Active unit JA and IG involvement.

(d) Codified responsibilities and requirements.

(e) Formally designated Program Monitor and alternate.

(f) Documented initial and annual training.

ENCLOSURE C

PROGRAM MONITOR CONTINUITY BINDER

1. The Program Monitor will maintain a non-DoD persons information protection continuity binder. The binder may be in electronic or hard copy format and will contain the following, at a minimum:

a. Appointment letters for primary and alternate Program Monitors.

b. Program Monitor duties and responsibilities.

c. Unit non-DoD persons information protection training.

d. Program training records (initial and annual).

e. Copies of references a and this instruction. Joint and ARNG programs must also have a copy of reference m.

f. Unit-oriented program self-inspection checklist.

g. Self-inspection and inspection records.

h. Annual file review certification MFR.

ENCLOSURE D

REFERENCES

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

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

c. CNGB Instruction 2000.01, 17 September 2012, "National Guard Intelligence Activities"

d. CNGB Manual 2000.01, 26 November 2012, "National Guard Intelligence Activities"

e. DoD SORN listing,<http://dpclo.defense.gov/privacy/SORNs/SORNs.html>, 21 June 2013

f. Executive Order 12333, 04 December 1981, "United States Intelligence Activities, (as amended by Executive Orders13284 (2003), 13355 (2004) and 13470 (2008))

g. AR 381-12, 04 October 2010, "Military Intelligence Threat Awareness and Reporting Program"

h. DoD Manual 5200.01-R Volume 4, 24 Feb 2012, "DoD Information Security Program: Controlled Unclassified Information (CUI)"

i. Privacy Act of 1974 (U.S.C. 552a)

j. NG Regulation 500-2, 31 March 2000, "National Guard Counterdrug Support"

k. NG Regulation 500-3/Air National Guard Instruction 10-2503, 09 May 2011, "Weapons of Mass Destruction Civil Support Team Management"

l. CNGB Instruction 0700.01, 09 June 2013, "Inspector General Intelligence Oversight"

m. AR 380-13, 30 September 1974, "Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations"

n. DoD 5400.11-R, 14 May 2007, "DoD Privacy Program"

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ANG	Air National Guard
AR	Army Regulation
ARNG	Army National Guard
AT/FP	Antiterrorism/Force Protection
CD	Counterdrug
CI	Counterintelligence
CIMS	Civil Support Team Incident Management System
CST	Civil Support Team
DoD	Department of Defense
DoJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
IAW	In accordance with
IC	Incident Commander
IG	Inspector General
IO	Intelligence Oversight
JA	Judge Advocate
JFHQ-S	Joint Force Headquarters-State
LE	Law Enforcement
LEA	Law Enforcement Agency
MFR	Memorandum for Record
MI	Military Intelligence
NG	National Guard
NGB	National Guard Bureau
PII	Personally Identifiable Information
PM	Provost Marshal
SAD	State Active Duty
SecDef	Secretary of Defense
SOP	Standard Operating Procedures
SORN	System of Records Notices
TAG	The Adjutant General
T-10	Title 10
T-32	Title 32

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.

Individual -- As defined by reference i, a citizen of the U.S. or an alien lawfully admitted for permanent residence.

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

National Guard Intelligence Component -- National Guard 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. National Guard 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, do not have to comply with federal intelligence oversight policies. In state active duty status, they are limited by state laws, to include state privacy laws. In most states, the collection, use, maintenance, and dissemination of U.S. persons information is strictly regulated; therefore, National Guard members in a state active duty status should seek competent legal advice on state laws before collecting information on U.S. persons.

Personally Identifiable Information -- As defined in reference p, 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. Rather, 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 whenever 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 -- Defined by reference i 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." A System of Records Notice is published in the Federal Register documenting the existence and content of the system of records.