OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

INTELLIGENCE COMMUNITY POLICY MEMORANDUM

NUMBER 2007-500-3

SUBJECT: (U) INTELLIGENCE INFORMATION SHARING

A. AUTHORITY: The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004; Section 303 of the Intelligence Authorization Act for Fiscal Year 2005; Federal Information Security Management Act of 2002; Clinger-Cohen Act, repealed and reenacted as 40 USC § 11101; Executive Order (EO)12333, as amended; EO 12958, as amended; EO 13355; EO 13388; and other applicable provisions of law.

B. PURPOSE:

1. This Intelligence Community Policy Memorandum (ICPM) establishes overarching policy to maximize intelligence information sharing within the Intelligence Community (IC) and with customers, identifies key elements that will govern implementation of the policy, and assigns responsibilities for ensuring that the policy is effectively carried out community wide. This memorandum also formally documents the roles and responsibilities of the IC Information Sharing Executive and of the Information Sharing Steering Committee (ISSC) chaired by the Information Sharing Executive (ISE).

2. This ICPM rescinds in part Director of Central Intelligence Directive (DCID) 8/1, Intelligence Community Policy on Information Sharing, leaving in effect the following three DCID 8 Series documents: (1) Policy Memoranda 1, Intelligence Community Implementation of Releasable by Information Disclosure Official Dissemination Marking; (2) Policy Memoranda 2, Modification to Policy for Non-Title 50 Organizations' Access to Shared IC Services on TS/SCI Information Systems; (3) Implementation Issuance Number 1, Guidelines for Tearline Reporting.

C. APPLICABILITY: This ICPM applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

D. POLICY:

1. The broadest possible sharing of intelligence information is fundamental to the mission of the IC. This responsibility, balanced by the obligations to protect national security information and the privacy and civil liberties of U.S. persons, is the guiding principle for all intelligence information sharing decisions. In applying this principle, the IC will be guided by mission requirements and the imperative to produce intelligence information usable by the widest appropriate audience.

2. Intelligence information is an asset of the Nation, not of a particular IC element. IC elements shall implement policies, procedures, processes, and training needed to end the practice of intelligence information "ownership" and implement the practice of intelligence information "stewardship" (see the list of definitions in Annex).

3. IC analysts shall have maximum and timely access to available intelligence information to ensure that policymakers and decision makers receive intelligence products that are based on intelligence information that has been collected or acquired by the IC.

4. To maximize the awareness, access, and dissemination of intelligence information within the IC, IC elements shall, consistent with national security requirements:

a. Enable the discovery (see Annex) of intelligence information to support personnel performing IC missions.

b. Provide maximum access to and dissemination of intelligence information (in the form initially gathered through the final form) while balancing the obligation of protecting intelligence sources and methods with the responsibility to provide intelligence information to meet customer mission requirements.

c. Apply DNI approved metadata tagging standards for all intelligence information (in the form initially gathered through the final form) to enable information discovery.

d. Apply proper classification and handling caveat markings to each portion of intelligence to enable intelligence information access and avoid improper disclosure or release.

5. To maximize the dissemination of intelligence information to IC customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall:

a. Produce intelligence products at the lowest level of classification possible or in an unclassified form, without losing meaning or essential context to meet customer requirements.

b. Implement DNI approved information technology, personnel/physical security standards, and procedures for providing and protecting intelligence information.

c. Implement a DNI approved attribute-based identity management capability to enable attribute-based access, user authorization, and user auditing services.

E. AUTHORITIES AND RESPONSIBILITIES:

1. The ISSC is an advisory body established to improve information sharing within the IC. ISSC members will work with the IC elements they represent in making recommendations to resolve intelligence information access and dissemination disputes. The ISSC shall:

a. Consist of a member from the offices of the Undersecretary of Defense for Intelligence, the Joint Chiefs of Staff Joint Staff, the Deputy Director of National Intelligence (DDNI) for Analysis, the DDNI/Collection, the DDNI/Policy, Plans, & Requirements, and each IC element.

b. Develop recommendations on intelligence information sharing issues and activities within the IC and to its customers.

c. Provide a collaboration and coordination venue for intelligence information sharing issues to include strategies, priorities, policies, procedures, guidance, necessary budgetary actions, and technical aspects for presentation to the DNI and the Executive Committee as required.

d. Develop, in coordination with relevant IC governance bodies, recommended IC positions on issues before the Information Sharing Council which supports the Program Manager Information Sharing Environment (PM-ISE) in meeting his information sharing responsibilities across the Federal government.

2. The IC Information Sharing Executive shall, subject to the direction of the DNI:

a. Provide overall leadership for all intelligence information sharing and dissemination initiatives.

b. Coordinate with the Program Manager-Information Sharing Environment on matters of mutual interest.

c. In coordination with appropriate Office of the Director of National Intelligence (ODNI) and IC elements, develop classification guidance to ensure appropriate uniformity, standardization, and consistency among IC elements in the classification of intelligence information.

d. Consistent with the obligation of the DNI to protect sources and methods and in coordination with appropriate ODNI and IC elements, develop and recommend for DNI approval IC guidance to ensure:

(1) Maximum access to and dissemination of intelligence information, in the form initially gathered through the final form.

(2) Preparation of intelligence products to meet customer requirements in such a way that sources and methods are protected, while retaining the meaning, to allow dissemination at the lowest level of classification possible or in an unclassified form to the extent practicable.

e. In coordination with appropriate ODNI and IC elements, and the ISSC, develop intelligence information sharing policies, processes, standards, practices, and training standards.

f. Develop or leverage existing intelligence information sharing services to enable intelligence integration and provide collaboration capabilities across multiple security levels.

g. Establish an IC inventory of intelligence information repositories.

h. Advise the Associate Director of National Intelligence and Chief Financial Officer on the development of the Intelligence Information Program budget inputs to implement intelligence information sharing policies, standards, processes, systems, training programs, and procedures across the IC.

i. In coordination with the IC and appropriate ODNI elements, establish performance measures for improved intelligence information sharing and track progress against these measures and the National Intelligence Strategy on an annual basis.

j. Report annual progress made in implementing this policy memorandum, to include any recommended actions, suggested policy, technology, or business process changes or resource adjustments to the DNI.

k. Monitor, track, and report, together with appropriate ODNI and IC elements, compliance with this policy directive.

l. In coordination with appropriate ODNI and IC elements, develop and issue training standards for DNI policies, guidance, and procedures related to intelligence information sharing, and oversee the implementation and execution of these IC training programs.

3. The Heads of IC elements shall:

a. Designate a representative to the ISSC who shall act as the intelligence information sharing focal point and spokesperson for their IC element. This representative will be responsible for issues related to intelligence information sharing and will identify and resolve intelligence information sharing issues within their IC element.

b. Ensure the production of intelligence products at the lowest classification level possible or in an unclassified form to meet customer requirements without losing meaning or essential context or jeopardizing intelligence sources and methods.

c. Develop supplemental supporting procedures, processes, tools, and training to implement this policy memorandum.

d. Educate and train their work force on IC intelligence information sharing policies, guidance, and practices.

e. Hold appropriate members of their organizations accountable for supporting this policy.

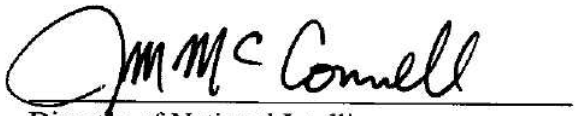
f. Include intelligence information sharing in the performance appraisal process as well as in award and recognition programs.

g. Include supporting goals, objectives, and performance measures in organizational strategic and performance plans, track progress against these measures, and report, on an annual basis, to the IC Information Sharing Executive, progress, and compliance with the same.

h. Provide an inventory of all intelligence information repositories under their purview to the IC ISE.

i. Ensure processes exist to facilitate sanitization of products to support time sensitive requirements.

F. EFFECTIVE DATE: This ICPM becomes effective on the date of signature. The relevant contents of this policy will be incorporated into an IC Directive.



Director of National Intelligence

22 DEC 07

Date

Annex - Definitions

Definitons, for purposes of this ICPM, are as follows:

1. Customer: A person or entity with whom intelligence information may be shared.

2. Discovery: The identification of the existence of information and a means to pursue obtaining that information but not necessarily having access to the information itself.

3. Intelligence Community Elements: Those agencies and elements listed as part of the Intelligence Community in Section 3(4) of the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

4. Intelligence in the Form Initially Gathered: The earliest point at which the recipient can make use of or add value to the information, or both.

5. Intelligence Information: Intelligence information includes the following information, in any medium, lawfully collected or acquired by an IC element: (1) foreign intelligence, counterintelligence, and intelligence information, as defined in the National Security Act of 1947, as amended, and in EO 12333, as amended; and (2) information describing U.S. intelligence and counterintelligence activities; sources and methods used for the acquisition, processing, or exploitation of intelligence; and any other data resulting from or relating to U.S. intelligence collection efforts.

6. Metadata Tagging: Uses encoded data that describes characteristics of information entities to enable identification, discovery, assessment, and management of the described entities.

7. Stewardship: The careful and responsible management of intelligence information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the same. In accordance with guidance established by this ICPM, the intelligence information steward provides maximum intelligence information access to elements of the IC and its customers, balanced by the obligations to protect national security information and the privacy and civil liberties of U.S. persons.