INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 501

DISCOVERY AND DISSEMINATION OR RETRIEVAL OF INFORMATION WITHIN THE INTELLIGENCE COMMUNITY

(EFFECTIVE: 21 JANUARY 2009)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; and other applicable provisions of law.

B. PURPOSE:

1. This Intelligence Community Directive (ICD) establishes in part the Director of National Intelligence (DNI) guidelines called for in Section 1.3(b)(9)(B) of EO 12333, as amended, addresses mandates in the Intelligence Reform and Terrorism Prevention Act of 2004 to strengthen the sharing, integration, and management of information within the Intelligence Community (IC), and establishes policies for: (1) discovery; and (2) dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC.

2. The overall objectives of this policy are to:

a. Foster an enduring culture of responsible sharing and collaboration within an integrated IC;

b. Provide an improved capacity to warn of and disrupt threats to the United States (U.S.) homeland, and U.S. persons and interests; and

c. Provide more accurate, timely, and insightful analysis to inform decision making by the President, senior military commanders, national security advisers, and other executive branch officials.

3. This Directive rescinds Intelligence Community Policy Memorandum (ICPM) 2007-500-3, *Intelligence Information Sharing*, 22 December 2007. The following three Director of Central Intelligence Directive (DCID) 8 Series documents remain in effect: (1) Policy Memoranda 1, "Intelligence Community Implementation of Releasable by Information Disclosure Official (RELIDO) Dissemination Marking;" (2) Policy Memoranda 2, "Modification to Policy for Non-

Title 50 Organizations' Access to Shared IC Services on TS/SCI Information Systems;" and (3) Implementation Issuance Number 1, "Guidelines for Tearline Reporting."

C. APPLICABILITY:

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended; and such other elements of any other department or agency as 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.

2. This Directive does not apply to purely law enforcement information. When law enforcement information also contains intelligence or intelligence-related information, this Directive shall apply to the intelligence or intelligence-related information.

D. POLICY:

1. IC elements shall treat information collected and analysis produced as national assets and, as such, shall act as stewards of information who have a predominant "responsibility to provide." In addition, authorized IC personnel have a "responsibility to discover" information believed to have the potential to contribute to their assigned mission need and a corresponding "responsibility to request" relevant information they have discovered.

2. *Responsibility to Provide.*

a. IC elements shall fulfill their "responsibility to provide" by making all intelligence and intelligence-related information (hereinafter referred to as "information") that IC elements are authorized to acquire, collect, hold, or obtain (hereinafter referred to as "information collected") or analysis an IC element is authorized to produce discoverable by automated means by "authorized IC personnel," in accordance with Section D, unless otherwise exempt in accordance with Intelligence Community Policy Guidance (ICPG) 501.1, *Exemption of Information from Discovery*. Authorized IC personnel are individuals identified by their element head and who have an appropriate security clearance and an assigned mission need for information collected or analysis produced. "Discovery," as defined in Appendix A, is the act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element.

b. "Stewards," as defined in Appendix A, shall fulfill their "responsibility to provide" by making all information collected and analysis produced by an IC element available for discovery by automated means by authorized IC personnel, unless otherwise determined by the DNI; by making as much information as possible available for automated retrieval upon discovery; and by presuming that authorized IC personnel who request information discovered possess a "need to know," in accordance with Section F.

3. *Responsibility to Discover.* "Authorized IC personnel," as defined in Appendix A, have a "responsibility to discover" information believed to have the potential to contribute to their assigned mission need. The act of discovery does not itself constitute a request for receipt of the information collected or analysis produced.

4. *Responsibility to Request.*

a. Authorized IC personnel have a corresponding "responsibility to request" relevant information they have discovered that has the potential to contribute to an analytic judgment, to optimize collection, to inform collection strategies and priorities, or to otherwise advance the

intelligence mission. Authorized IC personnel who have discovered information collected or analysis produced that is of possible relevance to their assigned mission shall meet in part their responsibility to request such information by taking affirmative steps to request such information collected or analysis produced from the appropriate steward in accordance with Section F if the content of the information is not already available.

b. Stewards shall determine whether authorized IC personnel who have discovered information collected or analysis produced, that may be relevant to an assigned mission need, and who have requested such information, may receive the information in accordance with procedures in Section F.

5. *Subsequent Use of Information.* Authorized IC personnel shall be responsible for the proper handling and use of information received from a steward. Use of information collected or analysis produced shall be in accordance with Section D.6. and ICPG 501.3, *Subsequent Use of Information.*

6. All IC personnel shall carry out their responsibilities under this Directive, including the discovery, dissemination, retrieval, and use of information collected or analysis produced, consistent with applicable law and in a manner that protects fully the privacy rights and civil liberties of all U.S. persons, as required by the Constitution, Federal statutes, Executive Orders, Presidential Directives, court orders, and Attorney General approved guidelines, including those regarding the dissemination of U.S. person information. In addition, the responsibilities under this Directive shall be carried out consistent with the Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information Sharing Environment.

7. To achieve the policy objectives in this Directive, the IC Information Sharing Executive (IC ISE) shall develop, in consultation with IC elements, integrated implementation plans that set forth required benchmarks each IC element head shall meet. Integrated implementation plans shall be subject to the approval of the DNI, after consultation with the Executive Committee (EXCOM).

a. These benchmarks shall serve as a minimum baseline and shall not be construed as fulfilling each IC element head's overall obligation to achieve the policy objectives set forth in this Directive in full and as quickly as possible.

b. At a minimum, stewards shall make disseminated analytic products discoverable by, and to the extent possible, available to authorized IC personnel by automated means as soon as possible, but no later than 1 June 2009.

8. Upon enactment of this Directive, IC elements shall ensure that new information technology (IT) systems or significant changes to existing IT systems provide the capability for discovery, dissemination, and retrieval of information collected or analysis produced through automated means. This requirement is not retroactive and shall be implemented in accordance with standards promulgated by the IC Chief Information Officer (IC CIO).

9. The Deputy Director of National Intelligence for Policy, Plans, and Requirements (DDNI/PPR), as the DNI's designee for policy, shall evaluate compliance with this policy as of 1 October 2009, and periodically thereafter, as determined by the DDNI/PPR or designee. Evaluation results shall be provided to the DNI and, at the DNI's discretion, to the EXCOM and others, as appropriate. An IC element that is unable to comply fully or is found to be in violation

of this policy shall report in writing to the DNI the reasons for failing to meet the objectives of this policy and the steps that will be taken to come into compliance.

E. DISCOVERY OF INFORMATION COLLECTED OR ANALYSIS PRODUCED:

1. *Collection Stewards and Analytic Production Stewards ("Stewards").*

a. IC element heads shall appoint one or more "collection steward(s)" for each type of collection activity the IC element is authorized to conduct, and shall appoint one or more "analytic production steward(s)" for all analytic activity it is authorized to conduct. Stewards shall be senior IC element officials.

b. Stewards shall make all information collected and all analysis produced by an IC element available for discovery by automated means by authorized IC personnel consistent with the requirements in Section D.6., including information collected through contracts, arrangements, agreements, or understandings. In some cases, this may mean that only standardized or limited metadata is made discoverable. In such cases, discovery requires that such information be described with sufficient detail to allow authorized IC personnel to make a reasonable determination regarding whether it is relevant to a mission need. In cases where content is not fully available, the steward shall provide instructions concerning how authorized IC personnel may request dissemination or retrieval of the content of the information collected or analysis produced.

c. Should an IC element head determine that discovery of information collected or analysis produced, or the confirmation of the mere existence of such information or analysis, will jeopardize the protection of sources, methods, or activities; compromise a criminal or national security investigation; or be inconsistent with the requirements in Section D.6., the IC element head may exempt such information or analysis from discovery unless and until such time as the DNI makes an exemption decision in accordance with ICPG 501.1.

d. IC elements that acquire or hold information provided by consent or by arrangement or agreement with federal departments; agencies; foreign nations or organizations; corporations; state, local, or tribal entities; or individuals outside the IC; shall seek to acquire or hold the information so as to authorize and provide discovery and dissemination or retrieval by authorized IC personnel, in a manner consistent with applicable Federal statutes, Executive Orders, Presidential Directives, court orders, and Attorney General approved guidelines.

2. *Authorized IC Personnel.*

a. Authorized IC personnel are U.S. persons employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, have a mission need for information collected or analysis produced by an IC element, and who have an appropriate security clearance. Authorized IC personnel shall be identified by their IC element head.

b. Until such time as an attribute-based identity management capability that enables automated user authorization, discovery, retrieval, and auditing services for IC personnel is approved by the DNI and implemented throughout the IC, IC element heads shall identify authorized IC personnel within their IC element who have discovery rights to information collected and analysis produced by other IC elements.

c. The total number of authorized IC personnel approved by stewards to retrieve information collected or analysis produced may be subject to the IC's ability to adequately audit such activities. The IC ISE, in coordination with relevant stakeholders, shall include an auditing capability as part of an integrated implementation plan, pursuant to Section G.1.a. (1) and (2), and shall advise the DNI of constraints on retrieval, if any. The IC CIO shall promulgate IT system standards to govern audit practices.

F. DISSEMINATION OR RETRIEVAL OF INFORMATION COLLECTED OR ANALYSIS PRODUCED:

1. Dissemination or retrieval of information collected or analysis produced shall be made available to authorized IC personnel through automated means in accordance with Sections D.2. and D.6. Legacy information should be made available for dissemination or retrieval in accordance with Section D.6., to the greatest extent practicable.

2. Upon discovery of information collected or analysis produced that authorized IC personnel believe may fulfill an assigned mission need, authorized IC personnel shall request the information from the appropriate steward. Stewards may designate certain information as pre-approved for automatic retrieval upon discovery. When seeking to obtain discovered information that the steward has not pre-approved for retrieval, authorized IC personnel shall provide the steward with information regarding their role, assigned mission need and when established, DNI approved identity attributes.

3. Stewards shall determine whether authorized IC personnel may retrieve or receive discovered information collected or analysis produced in accordance with this section.

4. Absent specific information to the contrary, stewards shall accept the information provided by authorized IC personnel, in accordance with Section F.2. above, as satisfying the "need-to-know" requirement. The steward may determine, based on specific, articulable facts, that the requestor's need for the information is significantly outweighed by the risks of providing it, using the risk management framework in Section F.5., or that providing the information would violate a statutory provision or a court order.

5. Stewards shall meet their responsibility to provide through a risk-managed approach when determining whether to permit the dissemination to or the retrieval by authorized IC personnel of the content of information collected or analysis produced. Stewards shall evaluate the risks associated with providing the content of information collected or analysis produced against the risks associated with denying the request and shall take special care to ensure determinations are made consistent with Section D.6.

a. Risks associated with providing information include, but are not limited to: risks to sources, methods, and activities; and risks of unauthorized or unintentional disclosure.

b. Risks associated with denying a request for information include, but are not limited to: risks to mission performance; and risks of incomplete or erroneous analytic judgments informing policy or other decisions.

6. In accordance with DNI guidelines, an IC element head may stipulate specific security and training requirements for authorized IC personnel to obtain the content of particularly sensitive discovered information. Such requirements shall be established as part of an integrated implementation plan developed and approved in accordance with Section D.7. and consistent

with Section D.6.and IC policy. IC element heads may not stipulate specific security or training requirements that exceed those imposed on their authorized IC personnel.

7. Should a steward deny the request, or partially deny the request (such as providing "minimized" content), authorized IC personnel who are not satisfied with the steward's determination may initiate a formal review through his or her Sensitive Review Board (SRB) in accordance with ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process.*

a. Stewards shall provide written justification for denial or partial denial of information to the requestor and appropriate SRBs, in accordance with ICPG 501.2.

b. The requestor's SRB and the steward's SRB shall attempt to resolve the dispute under the direction of the IC element heads. Disputes that cannot be resolved between SRBs shall be forwarded jointly by the affected SRBs to the DNI.

c. The DNI may resolve any risk management dispute that cannot be resolved at a lower level.

d. Disputes involving Attorney General approved guidelines, or court-ordered or statutory restrictions on the dissemination of information, such as dissemination of U.S. person information collected under the Foreign Intelligence Surveillance Act, shall be referred to the Attorney General if the dispute cannot be resolved by the DNI and affected IC element heads, in consultation with their General Counsels.

G. ROLES AND RESPONSIBILITIES:

1. The Office of the Director of National Intelligence (ODNI).

a. The IC ISE is the DNI's senior accountable official for the oversight and financial and program management of IC information integration efforts and shall:

(1) Develop a series of IC integrated implementation plans, in consultation with IC elements, and subject to DNI approval, that ensure all aspects of information sharing are addressed by the appropriate ODNI component or IC element, including but not limited to: IT architecture and standards; policies; human resource and cultural factors; business processes; information assurance; privacy; counterintelligence; risk management and security;

(2) Develop, in consultation with IC elements, a fully resourced, near-term, integrated implementation plan to achieve the policy objective in Section D.7.b.;

(3) Monitor implementation; identify, anticipate, and mitigate obstacles to implementation; and take appropriate steps to ensure any implementation plan developed pursuant to Section G.2.c. is appropriately resourced;

(4) Provide periodic progress reports to the DNI and the EXCOM;

(5) Provide subject matter expertise, as appropriate, to inform the development of IC policies in accordance with ICD 101, *IC Policy System*; ICPG 101.1, *IC Directives and Policy Guidance*; ICPG 101.2, *IC Standards*; and any other policy that may be promulgated pursuant to ICD 101;

(6) Implement, as appropriate, the dispute resolution process in accordance with ICPG 501.2;

(7) Assist the DDNI/PPR, as requested, in monitoring compliance and evaluating the effectiveness of this policy; and

(8) Create such committees, boards, or councils as the IC ISE deems necessary to carry out the responsibilities described herein.

b. The Chancellor of the National Intelligence University (NIU) shall, in coordination with IC elements, develop community-level information sharing training to promote understanding and individual responsibilities with respect to this Directive.

c. The IC CIO shall:

(1) Develop the IT architecture that supports this Directive;

(2) Develop and promulgate standards required to implement this Directive in accordance with ICPG 101.2, to include: documented procedures for the review and analysis of audit data to support security, counterintelligence, and intelligence oversight requirements; standards to allow information to be discoverable; and standards to define new or significant changes to existing IT systems in Section D.8.; and

(3) Maintain the list of designated stewards and authorized IC personnel.

d. The DDNI/PPR shall support policy requirements for implementation plans and shall evaluate and monitor compliance with this policy.

e. The IC Chief Human Capital Officer shall work with the Chancellor of the NIU to ensure information sharing education and training is mandatory for IC personnel and is linked to implementation of ICD 651, *Performance Management System Requirements for the IC Civilian Workforce*, and ICD 656, *Performance Management System Requirements for IC Senior Civilian Officers.*

f. The Deputy Director of National Intelligence for Collection and the Deputy Director of National Intelligence for Analysis shall work with stewards to develop a concept of operations to implement this Directive to inform the IT architecture and integrated implementation plans; and

g. The National Counterintelligence Executive shall provide a counterintelligence mission perspective to inform the IT architecture and any integrated implementation plans.

h. The Civil Liberties Protection Officer shall support IC elements in carrying out their responsibilities to implement this Directive in compliance with applicable requirements to protect privacy and civil liberties.

2. IC Element Heads shall:

a. Designate individuals in their IC element who are “authorized IC personnel.” Until such time as an attribute-based identity management capability exists for the IC, provide the list of positions and names to the IC CIO;

b. Name collection steward(s) and analytic production steward(s), and provide the list of positions and names to the IC CIO;

c. Produce a strategy to implement this policy and provide it to the IC ISE, including a specific, appropriately resourced plan to meet the objectives of this Directive;

d. Seek a DNI exemption from discovery for information collected or analysis produced, in accordance with the procedures in ICPG 501.1, when appropriate;

e. Appoint appropriate personnel from their element to SRBs in accordance with Section G.3.;

f. Ensure that new information systems or significant enhancements to information systems comply with Section D.8. of this Directive;

g. Provide assistance, as requested, to the DDNI/PPR in evaluating implementation of this policy;

h. Incorporate mandatory education to collectors, analysts, and others who collect, process, retain, or use information regarding the importance of information sharing in accordance with curriculum developed by the Chancellor of the NIU. Initial training of all relevant IC personnel shall be accomplished within six months after the curriculum is developed;

i. Negotiate arrangements, agreements, understandings, or commercial contracts that shall, to the greatest extent possible, seek to obtain terms that permit discovery, and dissemination or retrieval by authorized IC personnel; and

j. Provide authorized IC personnel in all IC elements specific training recommended by an IC element that is part of an integrated implementation plan, in accordance with F.6.

3. SRBs shall:

a. In accordance with implementation procedures set forth in ICPG 501.2, serve as their respective IC element head's designated body to resolve dissemination and retrieval disputes; and take proactive measures to help ensure information is made available to authorized IC personnel, as appropriate;

b. Be established within the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency, and the Federal Bureau of Investigation, with limited membership.

(1) The DIA SRB shall include at least one member from the intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, and represent the interests of the services;

(2) The ODNI SRB shall include a member from the National Reconnaissance Office; the Office of National Security Intelligence of the Drug Enforcement Administration; the Office of Intelligence and Counterintelligence of the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; the intelligence and counterintelligence elements of the Coast Guard; and represent the interests of these elements, as well as those of the ODNI.

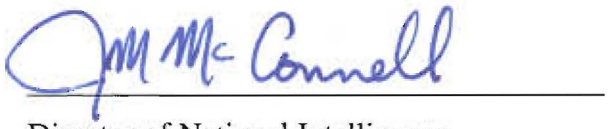
c. Consist of members cleared for access to all information, as determined by the DNI in consultation with IC element heads and in accordance with implementation procedures set forth in ICPG 501.2.

4. Stewards shall:

a. Make information collected and analysis produced available for discovery in accordance with this Directive; and

b. Make decisions with respect to information discovered and requested by authorized IC personnel in accordance with this Directive and pursue risk mitigation strategies to the greatest extent possible.

H. EFFECTIVE DATE: This ICD becomes effective on the date of signature.



Director of National Intelligence

21 JAN 09

Date

APPENDIX A - DEFINITIONS

ICD 501, DISCOVERY AND DISSEMINATION OR RETRIEVAL OF INFORMATION WITHIN THE INTELLIGENCE COMMUNITY

For the purposes of this Directive and all subordinate Policies and Standards, the terms below shall have the following meanings:

1. *Analysis Produced*: A disseminated or undisseminated product, assessment, study, estimate, compilation, or other report created and reviewed or validated by an IC element. It also includes databases comprised of information that may inform analysis. Databases become discoverable as part of a phased implementation plan in accordance with Section D.7.

2. *Authorized IC Personnel*: A U.S. person employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, has a mission need and an appropriate security clearance. Authorized IC personnel shall be identified by their IC element head and shall have discovery rights to information collected and analysis produced by all elements of the IC. The term may include contractor personnel.

3. *Collected*: Any information, both in its final form and in the form when initially gathered, acquired, held, or obtained by an IC element that is potentially relevant to a mission need of any IC element. This includes information as it is obtained directly from its source, regardless of whether the information has been reviewed or processed.

4. *Discovery*: The act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element. Discovery, as it is applicable under this Directive, is not defined or intended to be interpreted as discovery under the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, or other individual state discovery rules regarding non-privileged matter that is relevant to any party's claim or defense.

5. *Dissemination*: The act of a steward providing information collected or analysis produced by an IC element to authorized IC personnel, either through the ordinary course of business or in response to a request following discovery—(information "pushed" to authorized IC personnel).

6. *Information*: Intelligence and intelligence-related information. It does not include information pertaining to the internal administration or management of IC elements, such as IC personnel, medical, administrative, budget or security records.

7. *Intelligence*: As defined in EO 12333, as amended, includes foreign intelligence and counterintelligence.

8. *Mission Need*: A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Mission needs are determined by the mission and functions of an IC element or the roles and responsibilities of particular IC personnel in the course of their official duties.

9. *Retrieval:* The act of authorized IC personnel obtaining information collected or analysis produced by any IC element in response to a request following discovery through means other than dissemination.

10. *Steward (includes both Collection Steward and Analytic Production Steward):*

a. *Collection Steward*: An appropriately cleared employee of an IC element, who is a senior official, designated by the head of that IC element to represent a collection activity that the IC element is authorized by law or executive order to conduct, and to make determinations regarding the dissemination to or the retrieval by authorized IC personnel of information collected by that activity.

b. *Analytic Production Steward*: An appropriately cleared employee of an IC element, who is a senior official, designated by the head of that IC element to represent the analytic activity that the IC element is authorized by law or executive order to conduct, and to make determinations regarding the dissemination to or the retrieval by authorized IC personnel of analysis produced by that activity.

APPENDIX B – ACRONYM LIST

ICD 501, DISCOVERY AND DISSEMINATION OR RETRIEVAL OF INFORMATION WITHIN THE INTELLIGENCE COMMUNITY

CIO	Chief Information Officer
DCID	Director of Central Intelligence Directive
DDNI/PPR	Deputy Director of National Intelligence for Policy, Plans, and Requirements
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
EO	Executive Order
EXCOM	Executive Committee
IC	Intelligence Community
ICD	Intelligence Community Directive
IC ISE	Intelligence Community Information Sharing Executive
ICPG	Intelligence Community Policy Guidance
ICPM	Intelligence Community Policy Memorandum
IT	Information Technology
NIU	National Intelligence University
ODNI	Office of the Director of National Intelligence
RELIDO	Releasable by Information Disclosure Official
SRB	Sensitive Review Board
TS/SCI	TOP SECRET/Sensitive Compartmented Information