INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 500

DIRECTOR OF NATIONAL INTELLIGENCE
CHIEF INFORMATION OFFICER
EFFECTIVE: 7 AUGUST 2008

A. AUTHORITY: The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended; Section 303 of the Intelligence Authorization Act for Fiscal Year 2005; E-Government Act of 2002; Federal Information Security Management Act (FISMA) of 2002; Clinger-Cohen Act, repealed and reenacted as 40 U.S.C. § 11101; Federal Acquisition Streamlining of 1994; Executive Order 12333: United States Intelligence Activities, as amended; Government Performance and Results Act, Public Law 103-62, 31 USC 1115; Executive Order 12958: Classified National Security Information, as amended; Executive Order 13355: Strengthened Management of the Intelligence Community; Executive Order 13388: Further Strengthening the Sharing of Terrorism Information to Protect Americans, and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Directive (ICD) sets forth the authorities and responsibilities of the Chief Information Officer of the Intelligence Community. This ICD rescinds Director of Central Intelligence Directive 1/6, "The Intelligence Community Chief Information Officer."

C. APPLICABILITY: This directive applies to the Intelligence Community (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: The Chief Information Officer (CIO) within the Office of the Director of National Intelligence (ODNI) shall serve as the CIO of the IC and is designated by ICD 1 as an Associate Director of National Intelligence (ADNI/CIO).

1. In accordance with ICD 1, the ADNI/CIO is responsible for the overall formulation, development, and management of the IC's information technology (IT) enterprise required to implement the present and future business directives of the DNI. The ADNI/CIO will closely coordinate with the Department of Defense, Department of Homeland Security, Department of Justice and other U.S. Government Departments to produce compatible architectures, and common standards and policies ensuring the greatest transparency for intelligence support.

2. The ADNI/CIO shall be responsible for:

a. Providing advice and other assistance to the DNI and other senior management personnel in the ODNI to ensure that information technology is acquired and information resources are managed for the IC in a manner that implements the policies and procedures required by applicable law and the priorities established by the DNI;

b. Developing, maintaining and facilitating the implementation of a sound and integrated information technology architecture for the IC;

c. Promoting the effective and efficient design and operation of all major information resources management processes for the ODNI and for the IC, including improvements for work processes across the IC; and

d. Monitoring the performance of information technology programs of the IC, evaluating the performance of those programs on the basis of the applicable performance measurements, and, in coordination with other affected CIOs within the IC, advising the DNI regarding whether to continue, modify, or terminate a program or project.

3. In accordance with ICD 801, all major systems acquisitions that include the procurement of enterprise architecture-related IT items that are wholly or partially NIP-funded shall adhere to the applicable ADNI/CIO enterprise architecture, standards, protocols, and interfaces, and shall support the DNI's IC data and information sharing initiatives and shall be so certified. The ADNI/CIO, or the IC element or department CIO when Milestone Decision Authority (MDA) has been delegated in accordance with ICD 801 to the element or department, shall certify this compliance, as well as compliance with any other similarly applicable statutory provisions (such as the Clinger Cohen Act) to the MDA, as specified in ICPG 801.1.

4. Subject to the direction of the DNI, the ADNI/CIO shall support the information sharing strategies and policies of the IC.

5. In accordance with preceding subparagraphs 1 through 4, to ensure maximum availability of and access to intelligence information within the IC consistent with national security requirements as established by relevant law, policy, and directive; and to permit the DNI to protect intelligence sources and methods while maximizing the dissemination of intelligence, the ADNI/CIO shall, subject to the direction of the DNI, and in coordination with other CIOs within the IC:

a. Develop an enterprise architecture for the IC and ensure that elements of the IC comply with such architecture;

b. Direct and manage all Information Technology-related procurement for the IC in a manner that ensures that IC agency CIO's independent procurement and acquisition activities

and decisions undertaken in the execution of specific agency missions align to provide an integrated and interoperable framework across the IC to achieve the IC's strategic goals and information resources management goals as designated by the DNI;

(1) IC agency heads shall make procurement and acquisition decisions regarding exclusively internal agency systems that are designed to facilitate the conduct of agency operations and activities to support their statutory missions while ensuring there is no inconsistency with the IC's overall IT architecture and standards. The IC CIO shall be fully informed of such decisions, as he or she deems appropriate.

c. Execute, on behalf of the DNI and subject to his or her direction, procurement approval authority over all enterprise architecture-related IT items funded in the National Intelligence Program;

d. Consistent with ICD 801 and with paragraphs 2 and 5(b) and (c) above, have procurement approval authority over all IT items related to the enterprise architectures of all IC components;

e. Manage activities relating to the IT infrastructure and enterprise architecture requirements of the IC;

f. Establish common IT standards, protocols and interfaces for and within the IC;

g. Ensure development of IT systems within the IC that include multi-level security and intelligence integration capabilities;

h. Ensure that all expenditures for IT and research and development activities are consistent with IC enterprise architecture and the strategy of the DNI for such architecture;

i. In coordination with other responsible officials within the ODNI, and subject to the direction of the DNI, establish uniform information security standards and procedures for the IC to ensure IT infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy and directives;

j. Represent the DNI and the IC on the CIO Council;

k. With the concurrence of the Secretary of Defense or his or her designee, the Director Central Intelligence Agency or his or her designee, or other heads of agencies operating or exercising control of a National Security System, oversee IC information security policies and practices for national security systems as defined by FISMA as implemented and directed by the CIO's of agencies, offices, and elements of the IC, including:

(1) Developing and overseeing the implementation of policies, principles, standards and guidelines on information security, including timely adoption by all agencies, offices and elements of the IC standards promulgated for national security systems as authorized by law and directed by the President, and

(2) Requiring agencies, offices and elements of the IC, consistent with the standards promulgated for national security systems as authorized by law and directed by the President and

the requirements for information security established by Subchapter III of FISMA, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

(a) Information collected or maintained by or on behalf of agencies, offices and elements of the IC; or

(b) Information systems used or operated by or on behalf of an agency, office or element of the IC or by a contractor of an agency, office or element of the IC;

l. Identify issues that require IC Executive Committee attention and resolution and bring those issues to that committee for action; and

m. Perform other functions as the DNI may direct, or as indicated by applicable law.

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

J M McConnell

Director of National Intelligence

7 AUG 08

Date

APPENDIX A – ACRONYMS
ICD 500 – DIRECTOR OF NATIONAL INTELLIGENCE CHIEF INFORMATION OFFICER

ADNI/CIO	Associate Director of National Intelligence & Chief Information Officer
CIO	Chief Information Officer
DNI	Director of National Intelligence
FISMA	Federal Information Security Management Act
IC	Intelligence Community
ICD	Intelligence Community Directive
IRTPA	Intelligence Reform and Terrorism Prevention Act
IT	Information Technology
MDA	Milestone Decision Authority
ODNI	Office of the Director of National Intelligence