INTELLIGENCE COMMUNITY DIRECTIVE

NUMBER 700

PROTECTION OF NATIONAL INTELLIGENCE

(EFFECTIVE: 21 SEPTEMBER 2007)

A. AUTHORITY:

The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004; Executive Order (EO) 12333, as amended; EO 12958, as amended; EO 12968; and other applicable provisions of law.

B. PURPOSE:

This Intelligence Community Directive (ICD) establishes the Director of National Intelligence (DNI) security policy to protect national intelligence, as defined in section 1012 of the IRTPA, and intelligence sources and methods. It establishes the DNI's responsibilities for oversight and direction of IC security programs and activities. It also describes the roles and responsibilities of the Special Security Center (SSC), the Center for Security Evaluation (CSE), and Senior Officials of the Intelligence Community (SOICs), as defined by EO 12333, to protect our nation's secrets while enabling collaboration and information sharing, and eliminating unauthorized disclosures of national intelligence.

C. APPLICABILITY:

This directive 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 DNI and the head of the department or agency concerned, as an element of the IC.

D. POLICY:

1. The protection of national intelligence and intelligence sources and methods is fundamental to the success of the IC mission. IC security programs shall support the DNI's mission, protect national intelligence and intelligence sources and methods, foster a culture of information sharing, and effectively respond to evolving critical threats through proactive and integrated practices. SOICs, as the DNI's senior official for security matters within their organization, shall ensure security activities and programs support the National Intelligence Strategy, while detecting, neutralizing and defending against adversary attempts to degrade, manipulate, or destroy national intelligence capabilities. SOICs shall implement DNI guidance and employ clear, uniform, and reciprocal security policies and practices.

2. The DNI has the sole authority to create, modify or discontinue IC controlled access programs pertaining to national intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources and methods. Accordingly, SOICs shall adhere to the DNI process for the creation and management of controlled access programs and associated subcompartments.

3. Under the guidance of the DNI or his designee, SOICs are responsible for implementing DNI security guidance and are accountable for associated planning, programming, performance, and budgeting activities within their respective organizations.

E. AUTHORITIES AND RESPONSIBILITIES:

1. The DNI or his designee shall:

a. Protect national intelligence and intelligence sources and methods consistent with guidance from the DNI.

b. Establish and coordinate security policies and standards for the protection of national intelligence and intelligence sources and methods.

c. Coordinate with the DNI's Chief Information Officer to ensure the protection of national intelligence in the development of security policies and standards for information systems that store, process and communicate national intelligence.

d. Provide guidance for National Intelligence Program resources associated with security programs and activities and for the transfer or reprogramming of such resources as may be required.

e. Ensure the effective implementation of this policy collaboratively with IC elements, the National Counterintelligence Executive (NCIX) and all other relevant Office of the DNI (ODNI) entities.

f. Monitor the implementation and execution of security programs and activities.

g. Provide management oversight and direction to the security programs and activities that support the IC.

h. Ensure effective planning, programming and execution of security resources within the IC.

i. Establish fora for the identification and solution of issues affecting the protection of national intelligence and intelligence sources and methods.

2. The following ODNI centers shall report to and assist the DNI or his designee:

a. ***Special Security Center*** shall develop and coordinate DNI security policies and standards, in collaboration with the NCIX and the Chief Information Officer, for the protection of national intelligence and intelligence sources and methods. The SSC shall provide oversight and guidance for security policy implementation and provide services in security training, research, and database operation. The SSC shall interact with IC and national level security elements to ensure DNI equities and initiatives are properly considered in the development of national-level security policy and procedures.

b. ***Center for Security Evaluation*** shall ensure implementation of DNI security policies and guidance to protect classified national security information and operations, national intelligence, and intelligence sources and methods.

3. **Senior Officials of the Intelligence Community,** as the heads of departments and agencies with organizations in the IC or the heads of such organizations, as appropriate, shall:

a. ***Protect.*** Protect national intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the DNI.

b. ***Ensure Uniform Implementation.*** Implement uniform security policies and procedures in accordance with DNI directives and standards and ensure the proper protection, handling, storage and dissemination of national intelligence.

c. ***Promote Collaboration.*** Work together to identify and implement integrated responses to national security threats.

d. ***Ensure Security Reciprocity.*** Accept personnel security clearance background investigations and determinations completed by an authorized investigative agency or adjudicative agency and accreditations of information systems and facilities from other IC elements when there are no waivers, conditions or deviations to DNI security standards. Ensure that other elements receiving access determinations or accreditations are informed of all waivers, conditions or deviations to DNI security standards. The DNI shall be the final arbiter for all security reciprocity issues.

e. ***Manage Risk.*** Employ risk management processes to minimize the potential for compromise of national intelligence and intelligence sources and methods, while maximizing the sharing of information. These processes shall involve research and development of new tools and techniques to include cost effective countermeasures to counter threats and reduce vulnerabilities.

f. ***Ensure Access Criteria.*** Ensure the following criteria are met prior to providing access to classified information: (1) a favorable determination of eligibility for access has been made by an agency head, SOIC or their designee; (2) the individual has signed an approved non-disclosure agreement; and (3) the intelligence is needed to perform or assist in a lawful and authorized governmental function.

g. ***Support Counterintelligence Initiatives.*** Ensure security and counterintelligence elements work closely to ensure a collaborative approach to the protection of national security assets and national intelligence programs and activities.

h. ***Manage Insider Threat.*** Ensure all personnel with access to national intelligence are vetted, trained in their personal security responsibilities, advised of legal obligations and ramifications, and provided a secure work environment. SOICs shall implement aggressive security and counterintelligence initiatives to support the identification, apprehension, and, as appropriate, prosecution of those insiders who endanger national security interests.

i. ***Educate the Work Force***. Establish formal continuing security awareness, training and education programs to ensure complete, common and continuing understanding and application of IC security principles as contained in IC security directives. Individuals shall be indoctrinated and formally acknowledge their life-long security responsibilities and legal obligations to protect national intelligence.

j. ***Designate a Cognizant Security Authority (CSA).*** Designate a CSA to serve as the IC element authority for all aspects of security program management for the protection of national intelligence and intelligence sources and methods. CSAs may formally delegate this responsibility to specific elements within their organizations.

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

Director of National Intelligence

21 SEP 07

Date