INTELLIGENCE COMMUNITY DIRECTIVE NUMBER 502

INTEGRATED DEFENSE OF THE INTELLIGENCE COMMUNITY INFORMATION ENVIRONMENT (EFFECTIVE: 11 MARCH 2011)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; Executive Order 13526; and other applicable provisions of law.

B. PURPOSE

1. This Directive establishes policy on the integrated defense of the information environment for the Intelligence Community (IC). Integrated defense includes oversight, management, operations, and response activities within the IC, and in coordination with United States Government departments or agencies and other entities external to the IC. Integrated defense is essential to both information sharing and to the protection of sources and methods from unauthorized disclosure.

2. The IC information environment is defined as the individuals, organizations and Information Technology capabilities that collect, process or share Sensitive Compartmented Information, or that regardless of classification, are operated by the IC and are wholly or majority NIP-funded (e.g., DNI-U). The IC information environment is an interconnected shared risk environment where the risk accepted by one IC element is effectively accepted by all.

C. APPLICABILITY: 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.

D. POLICY

1. Integrated defense of the IC information environment is essential to maintaining the confidentiality, integrity, and availability of all information held by each IC element. Accordingly, the integrated defense of the IC information environment is critical to the execution of a unified, coordinated, and effective intelligence mission across the IC.

2. The Assistant Director of National Intelligence and IC Chief Information Officer (IC CIO) shall serve as the DNI designee for all matters pertaining to the integrated defense of the IC information environment. The IC CIO:

a. Shall develop and implement the *Concept of Operations for the Integrated Defense of the IC Information Environment* to establish a framework for developing unified courses of action to defend the IC information environment. The IC CIO shall coordinate, via established IC CIO governance structures, the development and issuance of the *Concept of Operations* no later than 180 days from the effective date of this Directive. Any IC Standards required for implementation of the *Concept of Operations* shall be developed in accordance with IC Policy Guidance 101.2, Intelligence Community Standards. Topics to be covered in the *Concept of Operations* include, but are not limited to:

(1) Procedures for defending the IC information environment from threats or incidents that could affect information sharing or the protection of sources and methods from unauthorized disclosure.

(2) Guidelines for the detection, isolation, mitigation, and response to incidents, which include spills, outages, exploits, attacks, and other vulnerabilities.

(3) Requirements for reporting incidents, spills, outages, configuration status, and other adverse events or vulnerabilities that affect the IC information environment of each IC element, and the IC information environment throughout the IC.

(4) Procedures for the coordination of the integrated defense of the IC information environment with IC elements; the Department of Defense; other U.S. Government departments and agencies; and other entities external to the IC, as appropriate.

(5) Standard operating procedures for the IC Incident Response Center (IC IRC), in the IC IRC's capacity as the IC center for the conduct of the integrated defense of the IC information environment.

b. Shall report to the DNI at least annually, by 1 June, on the status of the integrated defense of the IC information environment.

c. May establish IC Standards pursuant to this Directive, including IC Standards that address multi-level, cross-domain security solutions and minimum security standards for the IC information environment.

d. Shall establish IC Standards that address details specifying the implementation requirements of the Concept of Operations specified in Section D.2.a. The Standard(s) shall be developed consistent with IC Policy Guidance 101.2, Intelligence Community Standards.

3. IC elements shall:

a. Respond to the IC CIO with information required for the integrated defense of the IC information environment, except such information excluded under section 1.6(a) of Executive Order 12333.

b. Defend the IC information environment in accordance with this policy.

4. The IC IRC shall serve as the IC CIO's executive agent to monitor and oversee the integrated defense of the IC information environment. The activities of the IC IRC shall be in

accordance with the standards and guidelines implementing the *Concept of Operations* and shall include, but not be limited to:

a. Implementing and monitoring IC compliance with the *Concept of Operations* to ensure the integrated defense of the IC information environment.

b. Developing, maintaining, and sharing with IC elements situational awareness of network topology, including connection points among IC element networks; threats, vectors, and actions that could adversely affect the IC information environment; and the overall health and status of IC information environment defenses.

c. Coordinating activities for the integrated defense of the IC information environment with IC elements; the Department of Defense; and other U.S. Government departments and agencies, as appropriate.

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

Director of National Intelligence

11 MARCH 2011

Date