

Protection of National Intelligence



INTELLIGENCE COMMUNITY DIRECTIVE 700

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence (CI) Enhancement Act of 2002; Executive Order (EO) 12333, as amended; EO 13526; EO 12968, as amended; EO 13587; and other applicable provisions of law.

B. PURPOSE

1. This Directive establishes Intelligence Community (IC) policy for the protection of national intelligence, providing the framework for:

a. The protection of national intelligence and intelligence sources, methods, and activities; and the prevention of compromises, unauthorized disclosures, and misuses of national intelligence through coordinated CI and security activities;

b. Greater coordination and communication between CI and security activities of the IC to strengthen the ability to identify, deter, disrupt, mitigate, and counteract intelligence activities directed against United States (US) interests by foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities; and

c. Oversight of CI and security activities across the IC.

2. Intelligence Community Directive (ICD) 700, *Protection of National Intelligence*, dated 21 September 2007, is hereby superseded.

C. APPLICABILITY: This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to 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. National intelligence and intelligence sources, methods, and activities shall be protected. The integration of CI and security activities throughout the IC is the primary method for neutralizing threats by foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

2. CI and security shall be regarded as interdependent and mutually supportive disciplines with shared objectives and responsibilities associated with the protection of secrets and assets. CI gathers information and conducts activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. Security programs establish appropriate personnel, physical, information, operations, industrial and technical

security safeguards, and countermeasures to protect information and information systems, personnel, operations, resources, technologies, and facilities from threats.

3. Together, CI and security provide greater protection for national intelligence than either function operating alone. Integration does not require an organizational merging of CI and security offices; rather, integration facilitates the sharing of information, more efficient allocation of resources, and leveraging of authorities, competencies, and capabilities to enable and strengthen the protection of the US.

4. Therefore, CI and security functions shall be integrated, to the extent practicable, for the purposes of:

a. Protecting national intelligence and determining the eligibility of individuals to have access to national intelligence, sensitive information, and sensitive facilities, and to hold sensitive positions;

b. Enabling and supporting the identification, disruption, deterrence, and exploitation of foreign intelligence activities, including espionage, sabotage, and assassinations, both within the US and against US interests abroad;

c. Strengthening the deterrence, detection, and mitigation of insider threats, defined as personnel who use their authorized access to do harm to the security of the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of resources or capabilities;

d. Mitigating the risk of sabotage, compromise, or exploitation of the supply chain that could result in the surveillance, denial, disruption, or degradation of national intelligence capabilities;

e. Mitigating the risk of sabotage, compromise, or exploitation of the use of cyberspace to conduct intelligence activities against the US; and

f. Creating an environment which promotes a balance between the protection and sharing of national intelligence.

5. CI and security functions shall support the mission and enterprise objectives of the *National Intelligence Strategy* and the *National Counterintelligence Strategy of the United States of America*.

E. ROLES AND RESPONSIBILITIES

1. The DNI will:

a. Through the National Counterintelligence Executive (NCIX):

(1) Facilitate and monitor the implementation and effectiveness of IC CI and security policies, procedures, and programs, and develop recommendations for new or modified policies.

(2) Develop and promulgate IC CI and security standards and other guidance to implement IC CI and security policies.

(3) Provide guidance to IC elements on the development of budgets and spending plans associated with CI and security activities.

(4) Establish fora, as necessary, for the identification and resolution of issues related to the protection of national intelligence and intelligence sources, methods, and activities.

(5) Evaluate the effectiveness of IC CI and security activities; identify gaps, shortfalls, and resource needs; and recommend adjustments in allocations, additional resources, and other remedies to strengthen such programs across the IC.

(6) Establish and implement an inspection process for all US Government departments and agencies that handle national intelligence, to ensure those departments and agencies maintain effective operational security practices and programs directed against foreign intelligence activities.

b. Through the Assistant Director of National Intelligence and IC Chief Information Officer, protect national intelligence by ensuring information assurance and multi-level security capabilities are factors in establishing common information technology standards, protocols, and interfaces; and are considered in the development of national security systems for use in the IC.

c. Through the Assistant Director of National Intelligence for Human Capital, ensure the protection of national intelligence is considered in the development of standards and guidance for human capital activities.

d. Through the Assistant Director of National Intelligence and Chief Financial Officer, provide guidance for developing the CI and security portions of the consolidated National Intelligence Program budget, ensure the effective execution of the annual counterintelligence budget, and approve all transfers or reprogramming of such resources.

2. Heads of the IC elements shall:

a. Protect national intelligence and intelligence sources, methods and activities from unauthorized disclosure, consistent with federal laws, regulations, Executive Orders and any other applicable policy.

b. Ensure CI and security elements within their organizations collaborate and share data and information as necessary, to protect national intelligence and intelligence sources, methods and activities. For IC elements where either CI or security is a departmental asset, the IC element head is responsible for ensuring that any IC-related concerns are communicated to the Department.

c. Implement, where applicable, internal CI and security policies, procedures, practices, and programs in accordance with IC policies and standards to ensure the appropriate identification, protection, handling, storage, access to, and dissemination of national intelligence.

d. Employ risk management principles to minimize the potential for unauthorized disclosure or compromise of national intelligence and intelligence sources, methods, and activities while maximizing the sharing of information.

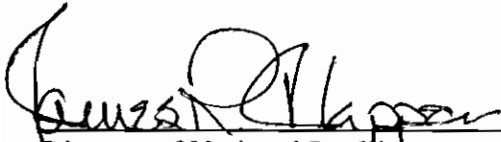
e. Ensure all personnel with access to national intelligence have: a need for access, a favorable determination of eligibility made by an authorized adjudicative agency, and a signed non-disclosure agreement. These personnel shall be continually evaluated and monitored, and regularly trained in their individual security responsibilities. They shall also be advised of legal and administrative obligations and the ramifications of a failure to meet those obligations.

f. Establish CI and security awareness, training, and education programs that provide a common understanding and application of CI and security policies and standards.

g. Provide programmatic, budgetary, and other relevant information as requested by the NCIX, to support the NCIX's CI and security responsibilities as described in Section E.1.a.5 above.

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

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



Director of National Intelligence

7 JUNE 2012

Date