INTELLIGENCE COMMUNITY DIRECTIVE 750

05 July 2013

(U) Counterintelligence Programs

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

B. (U) PURPOSE: This Directive establishes the baseline for CI programs across the Intelligence Community (IC) to create a strategic approach to CI that will enhance the national security posture of the U.S.

C. (U) APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned.

2. In cases where an IC element within a department is supported by the departmental CI program, the head of the IC element shall communicate the requirements of this Directive to the appropriate senior official and serve as an advocate and advisor for program development and implementation.

D. (U) DEFINITIONS

1. Counterintelligence: Information gathered and activities conducted 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.

2. Foreign Intelligence Entities (FIEs): Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

3. CI Programs: Capabilities and activities established within an organization for the purposes of identifying, deceiving, exploiting, disrupting, or protecting against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of FIEs.

4. Critical Asset: Any asset (person, group, relationship, instrument, installation, process, or supply at the disposition of an organization for use in an operational or support role) whose loss or compromise would have a negative impact on the capability of a department or agency to carry out

its mission; or may have a negative impact on the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may have a negative impact on the national security of the U.S.

E. (U) POLICY

1. (U/[redacted]) FIEs are engaged in highly sophisticated and persistent intelligence activities against U.S. interests. CI programs enable the U.S. Government to identify and neutralize these threats and therefore strengthen the national security posture of the U.S.

2. (U) CI programs enhance confidence in the intelligence provided to policy makers and other intelligence consumers, and mitigate FIE and insider threat efforts to influence or compromise U.S. plans, intentions, and capabilities.

3. (U/[redacted]) Effective mitigation of FIE activities involves anticipating, detecting, understanding, and assessing threats to national security and also taking appropriate CI actions to defeat, counter, neutralize, or exploit the threat.

4. (U/[redacted]) CI programs complement, use, support, and inform collection and analytic activities to identify vulnerabilities and protect national intelligence and intelligence sources, methods, and activities.

5. (U/[redacted]) CI programs provide CI analysis and CI awareness and education, and, as appropriate, provide risk assessments.

6. (U/[redacted]) CI programs enable and support the deterrence, detection, and mitigation of insider threats (as defined in the *National Insider Threat Policy*, dated 21 November 2012).

7. (U[redacted]) CI programs prioritize efforts to enable effective use and integration of CI and security resources by focusing on the mission objectives and threats outlined in the *National Counterintelligence Strategy of the United States of America* (hereafter *National CI Strategy*) and the *National Threat Identification and Prioritization Assessment*.

F. (U) IMPLEMENTATION

1. (U) IC element CI programs shall be:

a. Tailored to the distinct needs and missions of IC elements while adhering to the essential requirements described in Sections F.2 and F.3 of this Directive;

b. Functionally integrated with security programs, in accordance with IC Directive (ICD) 700, *Protection of National Intelligence*; and

c. In support of, and consistent with, the mission and enabling objectives of the *National Intelligence Strategy of the United States of America* and the *National CI Strategy*.

2. (U) IC element CI programs shall include:

a. (U/[redacted]) *CI analysis*: CI programs examine and evaluate information to determine the nature, function, interrelationships, personalities, and intent of FIEs, their agents, and insider threats that are targeting U.S. interests as an essential function of a CI program's ability to assess information of interest and provide threat briefings. CI analysis will conform to the analytic tradecraft and standards established in ICD 203, *Analytic Standards*. In cases where a CI analytic capability exists as a departmental function, the CI program within the IC element shall leverage those capabilities, as appropriate.

b. (U//[redacted]) *CI awareness and education*: CI programs provide information about foreign intelligence and insider threats to the U.S. and the IC, including indicators of an insider threat and targeting of U.S. critical assets including through cyber and other technical means. CI awareness and education programs demonstrate how rules regarding the use, sharing, storage, and destruction of classified or sensitive material and reporting requirements regarding personnel security, foreign contacts, foreign travel, and suspicious activities provide means to neutralize such threats.

c. (U//[redacted]) *CI risk assessments*: CI programs inform the evaluation of threats, identification of vulnerabilities, determination of adverse impacts, implementation of risk mitigation plans, and, as appropriate, sharing of information within and among interested parties including IC elements, members of the Executive Branch, and U.S. entities as defined in EO 13526, *Classified National Security Information,* Section 6.1(ss).

d. (U//[redacted]) *IC critical asset protection*: CI programs identify and heighten awareness of existing and emerging FIE threats to the IC element's programs, systems, facilities, personnel, and events to best protect those assets; therefore, CI programs shall be aware of critical assets that have been identified within the organization.

e. (U//[redacted]) *CI workforce competencies*: CI personnel shall have knowledge of foreign intelligence threats and tradecraft, insider threat detection and mitigation, cyber threats, and threats to the supply chain. Personnel assigned to CI programs shall have minimum competencies in accordance with standards on CI competencies issued pursuant to ICD 610, *Competency Directories for the Intelligence Community Workforce*.

f. (U) Other CI activities as directed and authorized by applicable statute or presidential directive.

3. (U) IC element CI programs shall be integrated with the following:

a. (U) Insider threat deterrence, detection, and mitigation. Consistent with the National *Insider Threat Policy* and the *Minimum Standards for Executive Branch Insider Threat Programs*, CI shall be integrated with security, user audits and monitoring, and other safeguarding capabilities within IC elements.

b. (U//[redacted]) Cyber threat awareness. CI shall be part of any IC element's efforts to defend the information environment and to identify and counter cyber threats. To facilitate the analysis or damage assessment of any external attempt to penetrate or compromise organizational information resources, IC elements shall ensure that CI programs are informed of any such attempt.

c. (U//[redacted]) Supply chain risk management. IC elements shall safeguard their supply chains from potential FIE exploitation or attacks by integrating CI programs into risk management efforts for acquisition and procurement programs.

G. (U) ROLES AND RESPONSIBILITIES

1. (U) The DNI, through the National Counterintelligence Executive (NCIX), will:

a. Conduct reviews of CI programs to evaluate the implementation of the *National CI Strategy*, consistent with ICD 700.

b. Produce and disseminate an annual report, based on the CI reviews discussed in Section G.1.a. The report will assess progress in meeting the objectives of the *National CI Strategy* and implementing this Directive. The report shall also include an overview and strategic assessment of IC CI activities, as informed by the information and notifications provided to the DNI by the heads of the IC elements in accordance with this Directive.

c. Establish IC CI interagency task forces, as needed, to develop strategic guidance for IC elements to identify and address emerging CI threats.

d. Promulgate IC Standards, in accordance with ICPG 101.2, *Intelligence Community Standards*, to provide additional guidance for IC CI programs.

e. Advocate for adequate resources to enable the IC elements to fully implement the *National CI Strategy*.

f. Research, identify, and share IC best practices, methodologies, and training programs to establish and maintain effective CI capabilities.

2. (U) Heads of IC elements shall:

a. Maintain a CI program for their element that is consistent with Section F of this Directive and applicable law, statute, and regulation within one year of the effective date of this Directive.

b. Designate a senior official responsible for the IC element's CI program.

c. Ensure their CI program supports the mission and enabling objectives of *the National Intelligence Strategy of the United States of America* and the *National CI Strategy*.

d. Ensure their CI program analyzes both external and internal attempts to penetrate or compromise organizational resources for potential ties to FIEs, and ensures prompt notification of any attempts to the senior official described in Section G.2.b, above.

e. Be responsive to requests by the DNI through the NCIX for information to enable the development of annual reports and Community-wide strategic CI priorities and objectives.

f. Ensure CI is incorporated into element insider threat programs in accordance with Section F.3.a of this Directive.

g. Ensure that CI considerations are incorporated into the agency's acquisition and procurement processes, to protect the supply chain.

h. Ensure that the training and professional development of personnel assigned to CI programs in the IC element are in accordance with the core performance elements and technical expertise competencies issued pursuant to ICD 610.

i. Ensure that all employees receive, at a minimum, initial CI awareness training within 30 days of entering on duty and annually thereafter.

j. Notify the NCIX upon commencement of a damage assessment relating to the perceived significant loss or compromise of intelligence information, operations, or assets.

k. Provide copies of Congressional notifications that relate to CI to the NCIX at the time they are provided to Congress and the ODNI Office of Legislative Affairs pursuant to ICD 112, *Congressional Notification*.

H. (U) EFFECTIVE DATE: This Directive becomes effective on the date of signature.

James R. Clapper
Director of National Intelligence

5 Jul 2013
Date