INTELLIGENCE COMMUNITY DIRECTIVE 710

21 June 2013

Classification Management and Control Markings System

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; EO 13526; EO 13556; 32 CFR Part 2001; and other applicable provisions of law.

B. PURPOSE

1. This Directive governs the implementation and oversight of the Intelligence Community (IC) classification management and control markings system, which provides the framework for accessing, classifying, disseminating, and declassifying intelligence and intelligence-related information to protect sources, methods, and activities.

2. This Directive supersedes Intelligence Community Directive (ICD) 710, *Classification and Control Markings System*, dated 11 September 2009; and rescinds Section IX of Director of Central Intelligence Directive (DCID) 6/6, *Security Controls on the Dissemination of Intelligence Information*. Sections I through IV and XI through XVI of DCID 6/6, DCID 6/5, and DCID 8 Series Policy Memoranda 1 were rescinded by ICD 710 in 2009.

C. 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. This Directive applies, pursuant to EO 13526, Section 6.2(b), to the handling of intelligence and intelligence-related information and, pursuant to EO 13556, Section 6(b), to the handling of unclassified intelligence or intelligence-related information (hereafter "intelligence information") that requires safeguarding through dissemination controls.

3. This Directive does not apply to information that is not intelligence or intelligence-related information, which may otherwise be protected by statute or presidential directive.

D. POLICY

1. Classification and Control Markings

a. Standardized classification and control markings are the primary means by which the IC protects intelligence sources, methods, and activities. The proper application and use of these markings enables information sharing while allowing the information to be properly safeguarded from inadvertent or unauthorized disclosure.

b. The IC markings system is implemented and maintained through the Controlled Access Program Coordination Office (CAPCO) *Register and Manual*.

(1) The CAPCO *Register and Manual* shall include all markings authorized for use with classified or unclassified intelligence information, as applicable, to communicate one or more of the following: classification type and level, controlled access programs, foreign government information, dissemination controls, disclosure and release determinations, and other warnings.

(2) Proposed new markings may be submitted to CAPCO by IC elements to accommodate national and IC policy requirements as well as operational needs.

c. Classification markings shall be explicitly and uniformly applied to classified intelligence information.

d. Control markings (as defined in Section E.2 below), when warranted, shall also be explicitly and uniformly applied to classified intelligence information and controlled unclassified information (CUI), consistent with guidance provided pursuant to EO 13526 and EO 13556. Unless originator consent is obtained, control markings shall be carried forward to any new format or medium which incorporates the information. To prevent information from being controlled unnecessarily, information that does not carry a dissemination control marking shall, to the maximum extent possible, not be combined within the same portion with information that requires a dissemination control.

e. If originator approval is required for further dissemination, the originator shall mark such requirement on the information, consistent with EO 13526, Section 4.1(i)(1).

(1) Classified intelligence information created on or after 28 June 2010 that does not bear such a marking may be further disseminated in accordance with EO 13526, Section 4.1(i)(1) and IC policy.

(2) Classified intelligence information created before 28 June 2010 that does not bear such a marking shall not be further disseminated without prior approval of the originator, unless the head or senior official of the originating IC element explicitly waived this requirement for specific information that originated within that element, in accordance with EO 13526, Section 4.1(i)(3), or unless the conditions listed in Section E.8 of ICD 703, *Protection of Classified Intelligence, Including Sensitive Compartmented Information*, have been met.

f. The lowest appropriate classification and least restrictive dissemination controls appropriate for that information shall be applied in order to maximize the dissemination, discovery, and retrieval of information.

g. Each section, part, paragraph, or similar portion (including the title and metadata) of a document containing classified intelligence information shall be marked to reflect the highest level of classification for that portion, or to reflect that the portion is unclassified. Portions of documents shall be marked, at the beginning of each portion, in a manner that clearly identifies the classification and applicable control markings for that portion. Additional guidance on portion markings is contained in the CAPCO *Register and Manual*.

h. Intelligence information transmitted over automated systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, and store classified information, shall conform to EO 13526 and 32 CFR Part 2001 for marking

electronic information and to IC standards and technical specifications on machine-readable classification and control markings.

i. When restrictive dissemination controls are applied to intelligence information, originators shall separate sources, methods, and activities content from the substantive classified intelligence information as appropriate using tearlines, write for release or other sanitization methods in accordance with ICD 209, *Tearline Production and Dissemination*, ICD 208, *Write for Maximum Utility*, and other applicable guidance.

2. Classification Management

a. Classification management includes controlling information throughout its life cycle and encompasses original classification, derivative classification, declassification, self-inspection, safeguarding, training, and oversight pursuant to EO 13526 and EO 13556.

b. Individuals designated, in writing, by an authority described in EO 13526, Section 1.3 have original classification authority (OCA). All others shall use derivative classification authority, defined as the use of source documents and security classification guides, to properly mark classified intelligence information.

c. All originally classified intelligence information shall include the classification level, identity (by either name and position or personal identifier) of the OCA, agency and office of origin (if not otherwise evident), declassification instructions, and a concise reason for classification. Intelligence information that is derivatively classified shall include the identifying information (by either name and position or personal identifier) for the derivative classifier, the appropriate derivative source(s) and appropriate declassification instruction.

d. Pursuant to EO 13526, Section 1.5(d), no information shall remain classified indefinitely. Generally, classified intelligence information shall be automatically declassified on 31 December of the year that is 25 years after the information was originally classified. The IC element head may exempt certain intelligence information from automatic declassification in accordance with EO 13526, Section 3.3.

e. When intelligence information no longer meets the standard for classification or otherwise needs to be declassified outside the automatic declassification process, the authority to do so, as outlined in EO 13526, generally rests with the OCA under Section 3.1(b) of the Order and with the agency head and senior agency official under section 3.1(d) of the Order. Declassification authority may be delegated in accordance with Section 3.1(b)(4). Pursuant to EO 13526, Section 3.1(c), the DNI, with respect to the IC, may declassify, downgrade, or direct the declassification of information or intelligence related to intelligence sources, methods, or activities after consultation with the head of the originating IC element or department.

E. IMPLEMENTATION: CLASSIFICATION AND CONTROL MARKINGS

1. A classification marking shall be applied to intelligence information only when the information requires protection from unauthorized disclosure and could reasonably be expected to cause identifiable or describable damage to national security.[1]

[1] Specific guidance on classification levels and appropriate markings is provided in EO 13526 and in 32 CFR Part 2001.

a. The classification markings permitted for use on classified information are TOP SECRET, SECRET, and CONFIDENTIAL. No other term or phrase shall be used to identify classified information. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

b. The UNCLASSIFIED marking may be used on intelligence information that does not meet the criteria for classification. The addition of controls to unclassified information shall be in accordance with national-level guidance provided pursuant to EO 13556, which will be reflected in the CAPCO *Register and Manual*, as appropriate.

2. Dissemination control markings identify the expansion of or limitation on the distribution of intelligence information. These markings (e.g., ORCON, IMCON, PROPIN, REL TO, RELIDO, NOFORN) are in addition to and separate from the levels of classification identified in Section E.1.a above. The CAPCO *Register and Manual* contains detailed guidance on the proper use of dissemination control markings. Authorized recipients who desire to disseminate intelligence information to additional users are encouraged to contact the originator of such information, through existing mechanisms, to request modification or removal of the dissemination control marking.

3. Foreign government information shall retain its original foreign government classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the foreign entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking, provided that the responsible agency determines that the foreign government markings are adequate to identify the level of protection required. Additional guidance on marking foreign government information can be found in the CAPCO *Register and Manual*.

4. Controlled Access Program markings shall be applied to information concerning or derived from intelligence sources, methods, activities, or analytical processes required to be handled within formal access control systems. Markings for controlled access programs shall be used in accordance with the CAPCO *Register and Manual*.

5. To facilitate the appropriate foreign disclosure and release of intelligence information, the following shall apply:

a. Originators shall explicitly mark classified disseminated analytic products with a foreign disclosure or release marking (i.e., NOFORN, REL TO, RELIDO, or DISPLAY ONLY);

b. Originators are encouraged to apply appropriate foreign disclosure markings as soon as practicable;

c. Classified disseminated analytic products that bear no explicit foreign disclosure or release marking shall:

(1) if created on or after 28 June 2010, be handled in the same manner as those documents that bear the Releasable by Information Disclosure Officer (RELIDO) marking; or

(2) if created prior to 28 June 2010, require an affirmative decision made by the originating agency's Senior Foreign Disclosure and Release Authority for foreign disclosure or release;

d. Other intelligence information that bears no explicit foreign disclosure or release marking shall be handled in accordance with the terms under which that information was made available. When possible, those terms should indicate the appropriate foreign disclosure or release marking; and

e. Foreign disclosure or release decisions shall be consistent with ICD 403, *Foreign Disclosure and Release of Classified National Intelligence*.

6. IC element heads may establish internal, administrative, and element-specific control markings for use on classified and unclassified intelligence information to meet unique mission needs. Such controls shall be consistent with existing policies and guidance and not duplicative of any markings in the CAPCO *Register and Manual*. IC element-specific internal controls shall not be used when information is disseminated outside that element.

7. The originating IC element may apply caveats or warnings to communicate distribution or handling instructions for the intelligence information; however, these caveats may not restrict dissemination beyond the restrictions already imposed by authorized control markings and must be consistent with any and all dissemination controls.

8. Authorized recipients of intelligence information who, in good faith, believe that a classification or control marking has been applied to information improperly are encouraged and expected to challenge the classification level or control marking.

a. Classification challenges shall follow procedures provided in Section 1.8 of EO 13526, as well as IC elements' implementing procedures established in accordance with that Order and pursuant to Section G.5.b of this Directive.

b. Control marking challenges shall follow procedures that IC elements establish pursuant to *DNI Guidance for Intelligence Community Marking Challenges* (NCIX 260-11, signed 18 January 2012).

9. Individuals granted access to classified intelligence information shall receive training, pursuant to EO 13526. This training shall ensure a complete and common understanding of the classification and control markings system.

10. CAPCO *Register and Manual* Review

a. The CAPCO *Register and Manual* shall be reviewed at least annually.

b. IC Elements shall incorporate any modifications to the CAPCO *Register and Manual* and machine-readable standards into IC automated systems that disseminate intelligence information within one year of the modification. IC systems shall be modified within one year to reject information not marked in accordance with the CAPCO *Register and Manual*, unless the National Counterintelligence Executive (NCIX) or designee approves a markings waiver or the IC Chief Information Officer (CIO) or designee approves a systems waiver.

c. During the implementation period for modifications described in Section E.10.b, the heads of the IC elements shall provide to CAPCO quarterly reports on the status of implementing the modification. Obstacles to implementation shall be noted in the report for possible ODNI waiver.

d. Immediate re-marking of legacy intelligence information shall not be required to reflect the current CAPCO *Register and Manual*. Such information shall only be re-marked with an updated classification or control marking upon its subsequent use or further dissemination.

11. The Classification Markings Implementation Working Group (CMIWG) shall serve as a standing IC forum to provide advice and guidance to the DNI on all matters related to the IC markings system, and to coordinate changes to the CAPCO *Register and Manual.*

12. The Classification Management Tool Working Group (CMTWG) shall serve as a standing IC forum to discuss and reach consensus on matters related to IC Classification Management Tool (CMT).

13. Markings oversight shall be accomplished through an annual report to the DNI through the NCIX on the use of classification and control markings on IC products. The annual report will evaluate and summarize the IC's implementation of ICD 710 and provide a basis to remediate and improve the IC markings system.

F. IMPLEMENTATION: CLASSIFICATION MANAGEMEMENT

1. Oversight of the classification management program shall be accomplished through annual self-inspections conducted by each IC element.

2. OCAs and other individuals delegated declassification authority in writing by the head of the IC element may declassify information within their purview pursuant to EO 13526 and 32 CFR Part 2001 guidelines. Only the DNI may declassify space-based national imagery, pursuant to EO 12951.

3. Training in classification management principles shall be conducted for original and derivative classifiers, consistent with EO 13526 and this Directive, and shall emphasize the avoidance of over classification and of unnecessary or overly restrictive dissemination control markings. IC elements may conduct additional training, as appropriate.

4. Safeguarding classified intelligence information and controlled unclassified information shall be the responsibility of all who have access to such information. Training in safeguarding procedures shall emphasize appropriate policies, procedures, and reporting criteria.

G. ROLES & RESPONSIBILITIES

1. The DNI:

a. Will maintain and update control markings to ensure that classified intelligence information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons, ensure the integrity of the information, and use common information technology (IT) standards;

b. Will serve as, and may delegate, OCA; and

c. May issue IC policy consistent with EO 13526, Sections 1.8(b) and 6.2(b).

2. The NCIX shall:

a. Maintain and oversee a process by which the heads of the IC elements may submit requests to modify the markings system. Requests shall be processed in coordination with IC elements and national entities as needed;

b. Oversee and ensure appropriate standardization of classification and control markings across the IC;

c. Approve requests for waivers to the markings, formats, or authorized abbreviations;

d. Resolve control marking challenges that cannot be resolved between IC elements;

e. Ensure that the CAPCO *Register and Manual* is accurate, current, and available to all users of classified and unclassified intelligence information;

f. Promulgate changes to the CAPCO *Register and Manual*;

g. Chair the CMIWG; and

h. Establish and manage the annual reporting process for classification and control markings, including coordination of the draft report with IC elements. Compile, draft, and deliver the annual report to the DNI.

3. The NCIX and the IC CIO shall:

a. Jointly establish and promulgate training standards for the control markings system and for classification management. The training shall emphasize the proper application of markings, principles of classification management, declassification, and, as necessary, CUI to ensure the protection of intelligence information and enable information sharing.

b. Serve as the points of contact for IC elements, departments and agencies of the executive branch, and the judicial and legislative branches for all matters relating to the IC control markings system and classification management.

4. The IC CIO shall:

a. Establish uniform IC procedures, architectures, IT standards, protocols, and interfaces to ensure that IC automated information systems:

(1) Prevent access to information by unauthorized persons or systems; and

(2) Maximize the availability of and access to information in a form and manner that facilitates its authorized use;

b. Update IC technical specifications to implement changes within 60 days of a CAPCO *Register and Manual* release;

c. Consider requests for waivers to systems implementation of markings, consistent with ICS 500-20, *Intelligence Community Enterprise Standards Compliance*;

d. Co-chair the Classification Management Tool Working Group (CMTWG) with the DNI-designated service provider of common concern for the CMT;

e. Establish and promulgate procedures for automatic declassification, as necessary;

f. Issue IC standards to support IC policy issued under Section G.1.c of this Directive, consistent with EO 13526, Section 1.8(b); and

g. Monitor IC element compliance, implementation, and reporting activities associated with EO 13526 and EO 13556 requirements.

5. Heads of IC Elements shall:

a. Ensure the classification and control markings system is implemented within their IC element, including through the establishment of procedures for the application of dissemination control markings and compliance with IC standards and technical specifications for machine-readable formats;

b. Provide IC element-specific classification and control markings implementation guidance to their workforce, including procedures for resolving marking challenges consistent

with *DNI Guidance for Intelligence Community Marking Challenges* (NCIX 260-11, 18 January 2012) and any other challenge guidance issued pursuant to this Directive;

c. Designate a primary and alternate point of contact to serve as the element's focal point for all classification management issues;

d. Delegate declassification authority, in writing, as appropriate;

e. Establish a program for periodic classification management and control markings training consistent with 32 CFR 2001.71, and standards issued pursuant to this Directive. The training shall emphasize the proper application of markings to enable information sharing while ensuring the appropriate protection of intelligence information;

f. Provide the DNI, through the NCIX, an annual report that summarizes the use of classification and control markings on their products and certifies that their workforce has been trained;

g. Submit requests in writing for waivers to the markings system, including portion marking waivers, to the NCIX or designee;

h. Provide the CMIWG and CMTWG with senior representative(s) who have experience with markings policy and technical implementation, the authority to represent their agency on matters related to the IC markings system, and the responsibility within their agency to implement the IC markings system;

i. Submit requests for new markings to CAPCO, in writing, via their CMIWG representative;

j. Provide the IC CIO with copies of self-inspection compliance reports. For IC elements within the Department of Defense, the Under Secretary of Defense for Intelligence shall provide the IC CIO with copies of self-inspection compliance reports; and

k. Ensure classification guides within their agencies are updated at least every five years, consistent with 32 CFR 2001.16.

6. OCAs shall:

a. Complete annual training consistent with EO 13526, this Directive, and standards issued pursuant to this Directive;

b. Appropriately apply classification markings, set a date or event for declassification, and provide appropriate contact information and declassification instructions; and

c. Downgrade or declassify intelligence information when it no longer meets the standard for classification.

7. Derivative Classifiers shall:

a. Complete training at least once every two years consistent with EO 13526, this Directive, and standards issued pursuant to this Directive;

b. Apply appropriate identifying information to all derivatively classified intelligence information;

c. Observe and respect original classification decisions by applying appropriate classification and control markings to all classified and controlled intelligence information;

d. Apply clear portion markings to the beginning of all required parts, paragraphs, or similar portions (including titles and metadata);

e. Observe and respect the decisions of the OCA; and

f. Challenge the classification status, if the derivative classifier believes that a classification status is improper, via procedures developed in accordance with EO 13526, Section 1.8 and pursuant to guidance provided in Section G.5.b of this Directive.

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

Director of National Intelligence

21 Jun 2013
Date