OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION 80.12
Category 80 – Information and Records Management
Office of Primary Responsibility: Assistant Director of National Intelligence for Policy and Strategy/Information Management Division
Revision 2

SUBJECT: CLASSIFICATION AND MARKING OF OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE INFORMATION

1. AUTHORITIES: The National Security Act of 1947, as amended; and other applicable provisions of law.

2. REFERENCES: Executive Order (EO) 13526; 32 CFR Part 2001; Intelligence Community Directive (ICD) 710, *Classification Management and Control Markings System*; the *Office of the Director of National Intelligence Classification Guide (ODNI CG)*; ODNI Instruction 10.03, *Director Of National Intelligence Delegation Of Original Classification Authority*; ODNI Instruction 80.16, *Office of the Director of National Intelligence Original Classification Authority*; and the *Intelligence Community Classification and Control Markings Register and Manual,* latest version.

3. PURPOSE: This Instruction provides guidance and establishes policy regarding the classification and marking of ODNI information. It also addresses the need to ensure personnel make proper classification determinations so that ODNI information is not only appropriately protected and properly marked, but also made readily available to our customers, where and when they need it. This Instruction replaces ODNI Instruction 80.12, *Classification of Office of Director of National Intelligence Information*, dated March 9, 2015.

4. APPLICABILITY: This Instruction applies to ODNI permanent cadre employees; ODNI staff reserve (i.e. time-limited) cadre employees, including Highly Qualified Experts; federal civilian detailees; military detailees; Intergovernmental Personnel Act detailees; Presidential appointees; assignees; and contractors.

5. POLICY: As original and derivative classifiers of ODNI information, all individuals have a responsibility to ensure national security information is properly marked and classified in accordance with EO 13526, 32 CFR Part 2001, the *IC Classification and Control Markings Register and Manual*, and the *ODNI CG*. Particular care should be exercised to avoid both over- and under-classifying ODNI information. When significant doubt exists about the need to classify information, it shall not be classified. When there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

A. **Classification:**

(1) Information eligible to be classified is addressed in eight categories outlined in EO 13526, and includes:

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) The development, production, or use of weapons of mass destruction.

(2) Information may not be classified to:

(a) Conceal violations of the law, inefficiency, or administrative error;

(b) Prevent embarrassment to a person, organization, or agency;

(c) Restrain competition; or

(d) Prevent or delay the release of information that does not require protection in the interest of national security.

(3) Information may be classified at one of three levels:

(a) Top Secret: When the unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security;

(b) Secret: When the unauthorized disclosure reasonably could be expected to cause serious damage to the national security; or

(c) Confidential: When the unauthorized disclosure reasonably could be expected to cause damage to the national security.

B. **Classification Authority:**

(1) Classification authority may be either original or derived. Refer to Instruction 80.16 for details on ODNI original classification authority (OCA). All individuals with access to classified information are authorized to apply derivative classification provided they have a valid need-to-know, signed a non-disclosure agreement, and received proper training regarding their responsibilities. Applying a derivative decision is accomplished by citing the applicable classification guide(s) or the specific source document. *The IC Classification and Control Markings Register and Manual* should not be used as a substitute for the *ODNI CG*. If classification guides do not cover a given situation, the information should be referred to the Classification Management Branch within the Policy & Strategy/Information Management Division (P&S/IMD) for guidance and resolution.

(2) A list of ODNI officials delegated OCA and their responsibilities are contained in Instruction 10.03. Original classification decisions made by these OCAs will be coordinated with IMD prior to implementation, to ensure timely updates to the *ODNI CG* and appropriate reporting requirements externally.

C. **Classification Markings:** Per EO 13526 and ODNI guidance, all classified information, and unclassified information with dissemination control markings, must be portion marked. This includes e-mail. All classified information, both hard copy documents and information produced through automated systems, must be marked in accordance with the *ODNI CG* and the requirements contained in the *IC Classification and Control Markings Register and Manual*. At a minimum, classified information must contain a banner that conspicuously displays the overall classification of the information residing therein; portion markings (to include paragraphs, sub-paragraphs, titles, charts, subject lines, etc.); date of origin; and a classification block to indicate the classifier, classification source, and duration of classification.

D. **Information Sharing and Dissemination:** Individuals should use restrictive markings such as NOFORN and ORCON ***as the exception*** rather than the rule. Per ICD 710, all classified disseminated analytic products (DAPs) must be appropriately classified and explicitly marked for foreign disclosure or release. For non-DAPs, explicit foreign disclosure and release markings are recommended, but not required. Individuals must coordinate foreign disclosure and release requirements for classified information with ODNI/Partner Engagement (PE) and with IMD Pre-Publication (email DNI-Pre-Pub) for unclassified information destined for release to foreign

partners. In all cases, the lowest appropriate classification and least restrictive dissemination controls applicable should be used.

E. **Working Papers**: Working papers, per 32 CFR Part 2001.24(d), are defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and if otherwise appropriate, destroyed when no longer needed. When any of the following conditions apply, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

(1) Released by the originator outside the originating activity (originating agency);

(2) Retained more than 180 days from the date of origin; or

(3) Filed permanently.

F. **Exceptional Cases**: When an individual who does not have OCA originates information believed by that person to require classification, he or she shall refer to sections 1.5, 1.6, and 1.7 of the *ODNI CG* and contact DNI-CLASSIFICATION for guidance.

G. **Classification Challenge Procedures:** Authorized holders of ODNI information who believe a classification decision is improper are *encouraged and expected* to challenge that classification using the procedures outlined in the *ODNI CG* and 32 CFR 2001.14. Prior to engaging in any formal classification challenge, individuals should first engage the author or sender of the information in question, or contact DNI-CLASSIFICATION for assistance.

H. **Training:** IMD is the focal point for classification training and will coordinate as necessary with ODNI offices to fulfill this requirement. Individuals designated as OCAs will receive mandated training when designated and on an annual basis thereafter. This training will be documented in an OCA Indoctrination letter and reported to the Director, Information Security Oversight Office (D/ISOO) as required by EO 13526. Individuals authorized to derivatively classify ODNI information will receive initial classification training within 30 days of arrival to the ODNI. ODNI cadre and military detailees also are required to complete annual refresher briefings via on-line web-based-training. Contractors must follow ODNI Contracts guidance, and government personnel detailed to the ODNI shall be guided by their respective parent agencies. Failure to comply with mandated training requirements may result in loss of classified network access, suspension of OCA or derivative classification authority, and/or other administrative action.

I. **Self-Inspection Program:** Pursuant to the provisions of EO 13526, the ODNI maintains a classification self-inspection program to assess the ODNI's compliance with the provision of EO 13526 and 32 CFR Part 2001. IMD is responsible for executing this program with oversight provided by the Chief Management Officer (CMO).

J. **Reporting Requirements:** Pursuant to sections 32 CFR Parts 2001.90 and 2001.91, the ODNI is responsible for a number of reporting requirements for which IMD will take the lead and coordinate as appropriate. These include reports to the ISOO covering:

(1) Delegations of OCA

(2) Statistical reports

(3) Classification management cost estimates

(4) Self-inspections

(5) Information declassified without proper authorization

(6) Reclassification actions

(7) Fundamental Classification Guidance Review

K. **Security Violations:** The CMO will notify the D/ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of EO 13526 that:

(a) Is reported to oversight committees in the Legislative branch;

(b) May attract significant public attention;

(c) Involves large amounts of classified information; or

(d) Reveals potential systemic weakness in classification, safeguarding, or declassification policy or practices.

L. **Penalties:** The penalties for misuse or mishandling of national security classified information are summarized in EO 13526, and other applicable provisions of law.

6. RESPONSIBILITIES:

A. The Chief Management Officer will:

(1) Provide policy oversight.

(2) Serve as the Senior ODNI Official per Section 5.4(d) of EO 13526 to direct and administer the ODNI classification management program.

(3) Ensure mandated training requirements established in EO 13526 and 32 CFR Part 2001 are accomplished and administrative or disciplinary actions are taken against personnel who do not comply, in accordance with paragraph 5.H. above.

(4) Notify the D/ISOO when a security violation occurs, in accordance with paragraph 5.K. above.

B. The Director, Information Management Division will:

(1) Establish and implement the ODNI's classification and automatic declassification programs under EO 13526, and exercise original classification authority according to Instruction 10.03.

(2) Create, maintain and promulgate the *IC Classification and Control Markings Register and Manual* and the *ODNI CG* and maintain a repository of other classification guides.

(3) Establish and implement ODNI classification and markings policy through the creation and maintenance of ICD 710, the *ODNI CG,* and other ODNI or IC-related guides.

(4) Provide easily accessible, relevant, and practical classification training and reference materials as required.

(5) Provide real-time, consistent, and accurate classification guidance for all types of ODNI information.

(6) Publish and update, as needed or required, in the Federal Registrar regulations concerning the handling of mandatory declassification review requests, to include the identity of the person(s) or offices(s) to which requests should be addressed, as required in 32 CFR Part 2001.33.

(7) Coordinate the ODNI response to classification actions, referrals, reporting requirements outlined in paragraph 5.J. above, challenges, mandatory declassification review requests, and appeals under EO 13526.

(8) Act as the Declassification Officer and liaison to the ISOO on all ODNI classification and declassification matters.

(9) Administer the ODNI's classification self-inspection program.

(10) Serve as classification system manager, supporting the Senior ODNI Official.

(11) Implement, as necessary, additional requirements contained in EO 13526 or as directed in ICD 710.

C. Component Directors, or designees, will:

(1) Ensure that all individuals in their components complete training on the proper classification and derivative classification of information to the level commensurate with their authorities and responsibilities, in accordance with paragraph 5.F above.

(2) Review and validate dissemination and distribution lists of classified information.

(3) Ensure that all component personnel are properly trained in handling and safeguarding ODNI classified information.

D. The Head of Contracting Activity will:

(1) Provide direction and oversight for mandated derivative classification training for ODNI contractors.

(2) Notify the D/IMD and the CMO of ODNI contractors who do not comply with mandated training requirements.

E. All individuals in the ODNI will:

(1) Properly classify and mark information as described in the *ODNI CG* and the *IC Classification and Control Markings Register and Manual.*

(2) Challenge the classification and markings of information if it is believed to be improper.

(3) Safeguard all sensitive and classified information entrusted to them.

(4) Immediately report to their supervisor any instances of known or suspected improper disclosure of classified information.

(5) Avoid over-classification.

7. EFFECTIVE DATE: This Instruction is effective upon signature.

Mark W. Ewing
Chief Management Officer

15 Jan 2016
Date