

(U) Application of Dissemination Controls: Originator Control

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

B. (U) PURPOSE

1. To provide direction and guidance for the application and use of the originator control marking (ORCON – the dissemination and extraction of information controlled by originator) to classified national intelligence.

2. The following are hereby rescinded:

a. Director of Central Intelligence Directive (DCID) 6/6, Section IX. B., *Dissemination and Extraction of Information Controlled by Originator*;

b. DCID 6/6, Annex A, *Guidelines for Use of the ORCON Caveat*;

c. Attachment A of Director of National Intelligence (DNI) Memorandum “Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with US Entities” (E/S 00045, 11 March 2011); and

d. *Sharing Classified National Intelligence*, PPR Memo (21 July 2010).

C. (U) APPLICABILITY

1. (U) This Intelligence Community Policy Guidance (ICPG) applies to the Intelligence Community (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 as an element of the IC by the President, or jointly by the DNI and the head of the department or agency concerned.

2. (U) This Guidance applies to the handling of classified national intelligence for the protection and responsible sharing of intelligence sources, methods, and activities information.

3. (U/[REDACTED]) This guidance applies to the dissemination of ORCON information that also contains sub-compartmented information within Human Intelligence and Special Intelligence Sensitive Compartmented Information control systems (such as Sensitive Source Reporting Program, Memorandum Dissemination, GAMMA sub-compartmented, National Security Agency Executive Series and I Series or reports disseminated under named distribution per the National Security Staff). Such



INTELLIGENCE COMMUNITY POLICY GUIDANCE 710.1

information shall also be handled in a manner consistent with the specified handling requirements for that sub-compartment in addition to the guidance for dissemination stipulated in Section E of this ICPG.

D. (U) POLICY

1. (U) Controls on the dissemination and use of classified national intelligence are necessary to protect intelligence sources, methods, and activities. The use of ORCON enables the originator to maintain knowledge, supervision, and control of the distribution of ORCON information beyond its original dissemination. Further dissemination of ORCON information requires advance permission from the originator. The ORCON marking shall be applied judiciously in accordance with this ICPG to ensure that classified national intelligence is disseminated appropriately without undue delay or restriction.

2. (U) The decision to apply ORCON shall be made on a case-by-case basis using a risk-managed approach. It shall not be applied in a general or arbitrary manner.

a. ORCON shall be applied consistent with the IC markings system and protocols established in the Controlled Access Program Coordination Office (CAPCO) *Authorized Classification and Control Markings Register and Manual*;

b. ORCON shall not be applied to unclassified information; and

c. ORCON shall not be used when access to classified national intelligence will reasonably be protected by the use of other appropriate classification or control markings.

3. (U) ORCON shall only be applied to classified national intelligence that meets one or more of the following criteria:

a. (U//) Classified national intelligence that clearly identifies or permits identification of intelligence sources, methods, or activities that are susceptible to countermeasures that would nullify or measurably reduce the effectiveness of the source, method, or activity; and where the classification level and other controls alone are insufficient to control dissemination;

b. (U//) Counterintelligence risk and vulnerability assessments that may require limited distribution;

c. (U//) Cybersecurity risk and vulnerability assessments that may require limited distribution;

d. (U//) Information used for the purposes of taking investigative, operational, or legal action;

e. (U//) Classified national intelligence or foreign government information that is required to be marked ORCON pursuant to interagency or intergovernmental agreements or a foreign intelligence arrangement, as a condition of passage. Future negotiations should seek to minimize the use of ORCON for such information, in accordance with Intelligence Community Directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*; and

f. (U//) Classified national intelligence, the unauthorized disclosure of which could prompt a foreign government or non-state actor to initiate counterintelligence activities.

4. (U) Requests for further dissemination of ORCON information and approval of such dissemination shall be based on a mission need of the intended recipient.

5. (U) Dissemination to Congressional committees shall be consistent with oversight functions and requirements.

6. (U) Consideration of requests for further dissemination shall use a risk-managed approach, by which the originator evaluates the benefits associated with providing the content against the risks associated with denying the request.

7. (U) Pre-approval decisions shall be made consistent with ensuring the maximum availability of and access to intelligence information, consistent with national security requirements. Originators shall, to the greatest extent possible, coordinate with intended recipients and product consumers (including offices that support dissemination to the Congressional oversight committees) to identify and pre-approve ORCON information for further dissemination beyond that which is authorized for the original product. Pre-approval decisions to further disseminate ORCON information should include consideration of the product line, mission area, means of dissemination, and additional recipients. IC element practices facilitating pre-approval of ORCON information for dissemination to the Congressional oversight committees shall be sustained and, as practicable, expanded.

8. (U) Reporting on the use of ORCON shall be included as part of the annual reporting requirements outlined in ICD 710, *Classification and Control Markings System*.

9. (U) The training conducted pursuant to both ICD 710 and EO 13526, Sections 1.3(d) and 2.1(d) shall include training on the proper use, application, safeguarding, processes for dissemination, and derivative use of the ORCON marking.

E. (U) IMPLEMENTATION

1. (U) Sharing of ORCON

a. Classified national intelligence bearing the ORCON marking may be shared with all components that have been authorized to receive the information via pre-approval or dissemination list;

b. Recipients of classified national intelligence that bears the ORCON marking may also share that intelligence without additional approval from the originator as follows:

(1) With components within their own organizations. Each IC element (as defined in 50 USC 401a) shall be considered a single organization;

(2) With their headquarters, defined as the organization that has authority, direction, and control over the recipient;

(3) With officials directly supporting the Secretary if the recipient is within a Department (as defined in 5 USC 101); and

(4) With Departmental components that function on behalf of the recipient (hereinafter, "subordinate components") and their immediate intelligence customers within their Department.

c. ORCON information to be shared under Section E.1.b, must be handled in accordance with requirements for access to classified national security information set forth in EO 13526, Section 4.1(a).

2. (U//) Recipients shall not take investigative, operational, or legal action based on information marked ORCON unless they have obtained permission from the originator in advance.

3. (U) ORCON in IC secure collaborative environments: Secure collaborative environments are virtual work environments involving two or more IC elements, with access controls that enable collaboration among authorized users.

a. (U//) Secure Communities of Interest (SCOI) are secure collaborative environments focused on specific regions or topics. The Principal Deputy DNI (PDDNI), in consultation with the heads of the IC elements, shall designate SCOIs within which relevant disseminated ORCON information originated by an IC element may be posted by any authorized recipient participating in the SCOI. Such consultation shall function as pre-approval, by the originators, for inclusion of their relevant ORCON within the SCOI. This consultation, and any resulting parameters, shall be recorded in a memo promulgated by the PDDNI;

b. (U//) The PDDNI may also establish secure collaborative environments that facilitate collaboration on a broad range of information not specific to a region or topic (such as A-Space);

(1) (U) The Deputy DNI for Intelligence Integration (DDNI/II) shall develop a Terms of Use (TOU) for each such secure collaborative environment in coordination with the IC elements. The TOU shall incorporate terms for the posting of ORCON information; and

(2) (U) Should a participant wish to post ORCON information that is not consistent with the TOU, that participant shall follow the existing procedures for requesting ORCON release.

c. (U) Participants are not authorized to share ORCON information outside a secure collaborative environment (including a SCOI) with any organization that is not otherwise an authorized recipient. Use of ORCON material outside of the environment shall be in accordance with the procedures in Section E.4.a; and

d. (U) All existing secure collaborative environments designated by the PDDNI shall be brought into compliance with the above within one year of the issuance of this guidance. Pending completion of that action, the posting of ORCON information within these existing environments remains authorized consistent with their establishing documentation.

4. (U) Requests for pre-approval:

a. Analytic products that incorporate ORCON information in whole or in part may be disseminated only to originally authorized recipients of the ORCON information, unless the originator has approved the ORCON information for further dissemination. Authorized recipients are defined as those included within the dissemination list combined with those users described in Section E.1.b;

b. Pre-approval of ORCON information shall be demonstrated through the amendment of the distribution list or inclusion of the specific pre-approval agreement at the beginning of the

ORCON information. The pre-approval shall be presented in a manner that clearly states for whom the information is pre-approved and that is both visible in electronic and hard-copy versions of the document and is machine and human-readable for all versions of the document; and

c. Requests for further sharing of ORCON information may include recipients outside the IC provided that recipients meet the access requirements set forth in EO 13526, Section 4.1(a). Further dissemination by those recipients requires originator approval.

5. (U) Originators shall provide a written justification to the requestor for the denial or partial denial of a request for pre-approval or for further dissemination.

6. (U) Dispute resolution: The process and timeline described in ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process*, shall be used for resolving disputes related to the denial to retrieve ORCON information. Recipient agencies may ultimately appeal denials by the originating agency for further dissemination of classified national intelligence, including pre-approval requests, to the DNI or his designee.

7. (U) Challenges: Recipients may challenge the application of the ORCON marking in accordance with *DNI Guidance for Intelligence Community Marking Challenges* (NCIX 260-11, 18 January 2012).

F. (U) ROLES AND RESPONSIBILITIES

1. (U) The DNI will:

a. Through the PDDNI, in consultation with the heads of the IC elements, designate secure collaborative environments authorized for ORCON;

b. Through the IC Chief Information Officer:

(1) Promulgate an IC Standard that facilitates the technical dissemination of ORCON information. This Standard will cover common processes, nomenclature, metadata requirements, standard pre-approval and distribution list constructs, and other technical criteria, as appropriate; and

(2) Maintain a list of designated secure collaborative environments.

c. Through the National Counterintelligence Executive (NCIX):

(1) Issue standard criteria describing the training requirements in accordance with Section D.9;

(2) Establish a website on a classified network that makes available Point of Contact (POC) information, directions for ORCON dissemination requests, and any additional information that facilitates the sharing of ORCON (for example, links to lists, forms, and procedures) provided by originators in accordance with Section F.3.b; and

(3) Provide metrics on the use of ORCON including the potential misapplication of ORCON to the DDNI/II and IC Information Sharing Executive, at least annually.

2. (U) Heads of IC Elements shall:

a. Respond to pre-approval and further dissemination requests in accordance with the terms of this guidance;

- b. Identify to the DNI, within 90 days of the effective date of this guidance, their headquarters element and subordinate components, consistent with Section E.1; and
 - c. Establish ORCON training consistent with this policy and in accordance with the standards established in accordance with Sections D.9 and F.1.c.(1).
3. (U) Originators of ORCON information shall:
- a. (U) Coordinate with intended recipients and consumers (including IC offices that support dissemination to the Congressional oversight committees), applying a risk-managed approach to identify the widest appropriate dissemination of ORCON information;
 - b. (U) Provide the DNI, through the NCIX, with POC information, directions for ORCON requests, and any additional information that facilitates the sharing of their ORCON information (for example, links to lists, forms, and procedures);
 - c. (U) When the ORCON marking is used, separate sources, methods, and activities content from the substantive classified national intelligence by using tearlines, write for release, or other sanitization methods, in accordance with DNI policy;
 - d. (U) Coordinate with the DDNI/II on the TOU for secure collaborative environments;
 - e. (U) Identify an electronically accessible form for processing all ORCON pre-approval and further dissemination requests. This form shall have the capability to document both requests and decisions, as well as capture metrics on approvals and denials of pre-approval and further dissemination requests; if such a form cannot be created, establish an analogous process for these functions and information (for example, an e-mail account);
 - f. (U) Review, within three days of receipt, all requests for the further dissemination of ORCON information. The originating agency must communicate its decision or its justification for extending the timeline for a decision (generally not to exceed seven days) to the requesting agency. This period may be extended if the requesting agency specifies a longer period of time for a response or as otherwise authorized by the DNI;
 - g. (U//) For requests that are time critical and require immediate action on the cleared information (e.g. immediate analytical assessment, diplomatic intercession, military operation, arrest/detention, or National Terrorism Advisory System alert), provide a response as soon as possible and not later than 24 hours. A justification is required for all requests that require the originator to respond within such a critical timeframe. This timeframe also applies to immediate or urgent requests on behalf of Congressional oversight committees. For those requests where it is necessary to disseminate ORCON information to respond to an imminent threat to life or in defense of the homeland, and a response is required in less than eight hours, requestors shall consider this situation an emergency in accordance with the terms of Section 4.2(b) of EO 13526;
 - h. (U) Adhere to the timelines and processes outlined in ICPG 501.2 for disputes related to requests for the further dissemination or pre-approval of ORCON;
 - i. (U) Adhere to the timelines and processes outlined in the *DNI Guidance for Intelligence Community Marking Challenge Procedures*; and

j. (U) Complete training on the proper use of ORCON, safeguarding of ORCON information, and processes for release.

4. (U) Recipients and requestors:

a. Shall submit pre-approval or further dissemination requests if the recipient has identified other customers who will require or benefit from the ORCON information;

b. Shall submit requests as soon as possible, using the originator's electronically accessible request form or analogous means for ORCON requests. These requests must include:

(1) The requestor's justification, including the mission need of the intended recipient; and

(2) The identification of all proposed uses and recipients, by agency.

c. Shall formally document, in an electronically accessible form, the further dissemination of ORCON information including dissemination via e-mail and report metrics to the originator and the DNI annually;

d. Shall adhere to the timelines and processes described in ICPG 501.2 for disputes related to the implementation of this guidance; and

e. Shall report any potential misapplication of ORCON to the Office of the NCIX.

G. (U) DEFINITIONS

1. Pre-approval: Authorization by the originator that permits further dissemination of the information beyond the initial distribution list. The originator may identify a user, set of users, or type of use for this information or may pre-approve new users as a result of requests made on behalf of new recipients.

2. Further Dissemination: Dissemination of ORCON information beyond the initial dissemination list or those entities listed in Section E.1.b. Further dissemination may only occur as a result of originator permission or pre-approval.

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



Director of National Intelligence

25 JULY 2012

Date