NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY MANUAL 1-52

Issue Date: 30 September 2013
Revised: 22 October 2013

NSA/CSS CLASSIFICATION GUIDE

PURPOSE AND SCOPE

In accordance with NSA/CSS Policy 1-52, "Classified National Security Information" (Reference a), this manual imposes special requirements to *classify*, *declassify*, *safeguard*, and *mark classified national security information*. It implements Reference a, Executive Order 13526, "Classified National Security Information" (Reference b), and other implementing documents (References c-f).

In implementing E.O. 13526 (Reference b), this manual reflects the principle that protecting information critical to national security and demonstrating commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective *declassification* are equally important priorities.

KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS

Endorsed by
Associate Director for Policy

DISTRIBUTION:
DJ2
DJ1
DJ6 (Vital Records)
DJ6 (Archives)

This Policy Manual supersedes NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual," dated 8 January 2007 and Policy Memorandum 2013-02, "Classification Challenges – Amendment to Policy Manual 1-52," dated 3 May 2013.
OPI: Information Security Policy, DJ2, 963-2882s.

Policy Manual 1-52 is approved for public release.

The Chief, Corporate Policy approved an administrative update on 22 October 2013 to clarify that if a single portion of a document contains controlled unclassified information then the entire document must be portion marked (see paragraph 4.2 of Annex A).

TABLE OF CONTENTS

1. ORIGINAL CLASSIFICATION

1.1. Classification Standards

1.1.1. Information may be originally classified only if all of the following conditions are met:

1.1.1.1. An *original classification authority (OCA)* is classifying the information;

1.1.1.2. The information is owned by, produced by or for, or under the control of the U.S. Government;

1.1.1.3. The information falls under one or more of the following categories:

(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 national security;

(f) U.S. Government programs for safeguarding nuclear materials or facilities;

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

(h) the development, production, or use of weapons of mass destruction; and

1.1.1.4. The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in *damage to national security* and the OCA is able to identify or describe the damage.

1.1.2. If there is significant doubt about the need to classify information, it shall not be classified.

1.1.3. Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

1.1.4. The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

1.2. Classification Levels

1.2.1. Information may be classified at one of three levels based on the degree of damage to national security that reasonably could be expected if the information were disclosed without authorization.

1.2.1.1. "TOP SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe;

1.2.1.2. "SECRET" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the OCA is able to identify or describe; and

1.2.1.3. "CONFIDENTIAL" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the OCA is able to identify or describe.

1.2.2. If there is significant doubt about the appropriate level of *classification*, it shall be classified at the lower level.

1.2.3. Information that is unclassified may be withheld from the public for one or more of the reasons cited in the Freedom of Information Act (Reference g), exemptions 2 through 9 and will be considered FOR OFFICIAL USE ONLY (FOUO). FOUO protection is afforded to information such as the names of NSA/CSS employees and certain missions and functions. This category of information may also be referred to as controlled unclassified information. Further guidance can be found in NSA/CSS Policy 1-5, "NSA/CSS Freedom of Information Act Program" (Reference h).

1.3. Classification Authority

1.3.1. *Original classification* is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only an OCA may classify information originally. Within NSA/CSS, there are currently 22 individuals designated as OCAs ("*go oca*"). In the absence of an OCA, a person trained as an OCA and that the OCA designates in writing may act on his or her behalf.

1.3.2. Original classification decisions are only required in those instances where the information is not covered by existing classification guidance such as is available in a *classification guide* or *declassification guide*, or any other form of documented OCA decision(s) (e.g., a decision documented in a Staff Processing Form (SPF)).

1.3.3. An OCA decision may only be made by an OCA with jurisdiction over the information. For each original classification decision, the OCA must ensure the information meets the standards for classification identified in section 1.1 and is not limited or prohibited from classification (see section 1.6.1). The OCA determines the appropriate classification level (see section 1.2), foreign releasability instructions, and any other handling instructions or *markings*, and determines the duration of classification in accordance with section 1.4. OCA decisions must be endorsed by the Associate Director for Policy and Records (ADPR), or designee, prior to implementation.

1.3.4. When a person originates information he or she believes to require classification, the information shall be protected in a manner consistent with this guide. The information shall be provided promptly to an OCA with purview over the information. The OCA shall decide within 30 days whether to classify the information.

1.4. Duration of Classification

1.4.1. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an OCA shall follow the sequence in this section when determining the duration of classification of originally classified information.

1.4.1.1. The OCA shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

1.4.1.2. If unable to determine a date or event of less than 10 years, the OCA shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

1.4.1.3. If unable to determine a date or event of 10 years, the OCA shall assign a declassification date not to exceed 25 years from the date of the original classification decision.

1.4.1.4. In those rare cases where NSA/CSS has been granted an exemption, the OCA will assign a declassification date that is 50 years from the date of the original classification decision. See section 4.2.1.1.2.

1.4.2. Extensions of classification are not automatic.

1.4.2.1. If the date or event assigned by an OCA has not passed, an OCA with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date or origin of the record.

1.4.2.2. If the date or event assigned by the OCA has passed, an OCA with jurisdiction over the information may reclassify the information in accordance with Executive Order 13526 (Reference b).

1.4.2.3. When extending the duration of classification, the OCA must be an OCA with jurisdiction over the information, ensure that the information continues to meet the standards for classification as stated in section 1.1, and make reasonable attempts to notify all holders of the information.

1.4.3. Unless declassified earlier or the duration of classification has been extended as described in section 1.4.2, information marked with a specific date or event for declassification is subject to automatic declassification (see section 4.2.1.1).

1.4.4. No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, or classified information that contains incomplete declassification instructions or lacks declassification instruction shall be declassified in accordance with the *automatic declassification* provisions of Executive Order 13526 (Reference b). Declassification Services (DJ5) manages this function for NSA/CSS.

1.5. Identification and Markings

1.5.1. At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

1.5.1.1. One of the three classification levels defined in section 1.2.1;

1.5.1.2. The identity, by name and position, or by personal identifier, of the OCA;

1.5.1.3. The agency and office of origin, if not otherwise evident;

1.5.1.4. Declassification instructions, which shall indicate a date consistent with guidance in section 1.4.1.

1.5.1.5. A concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.1.1.3.

1.5.2. Specific information required by section 1.5.1 may be excluded if it would reveal additional classified information.

1.5.3. The originator of a document shall, by marking or other means, indicate which portions are classified (with the appropriate classification level) and which portions are unclassified.

1.5.4. See Annex A for additional guidance on markin g.

1.5.5. Foreign government information (FGI) shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. FGI 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 meet the purposes served by U.S. classification markings. Details on marking foreign government information can be found in References e and f.

1.5.6. Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the *derivative classification* process or is reviewed for possible declassification, holders of such information shall coord inate with an appropriate classification authority for the application of omitted markings.

1.5.7. The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unc lassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in an unclassified form.

1.5.8. Prior to public release, all declassified records shall be appropriately marked to reflect their declassification .

1.6. Classification Prohibitions and Limitations

1.6.1. In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

1.6.1.1. Conceal violations of law, inefficiency, or administrative error;

1.6.1.2. Prevent embarrassment to a person, organization, or agency;

1.6.1.3. Restrain competition; or

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

1.6.2. Basic scientific research information not clearly related to national security shall not be classified.

1.6.3. Information may not be reclassified after declassification and release to the public under proper authority unless it meets the criteria in section 1.7(c) of E.O. 13526 (Reference b).

1.6.4. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (Reference g), the Presidential Records Act (Reference i), the Privacy Act (Reference j), or the mandatory declassification review process (Reference k). This may only occur if such classification meets the requirements in this policy and is accomplished on a document-by-document basis with the personal involvement of the *Senior Agency Official*. The requirements of this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an OCA in accordance with section 1.4.

1.7. Compilation of Information

1.7.1. A compilation of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that meets the standards for classification (section 1.1) and is not otherwise revealed in the individual items of information. Similarly, a compilation of items of classified information may be classified at a higher level if the compiled information reveals an additional association or relationship that meets the standards for classification and is not otherwise revealed in the individual items of classified information.

1.7.2. A compilation of items of information that are individually unclassified may be marked as UNCLASSIFIED//FOR OFFICIAL USE ONLY if the compiled information may be withheld for one or more of the reasons cited in exemptions 2 through 9 of the Freedom of Information Act (Reference g).

2. DERIVATIVE CLASSIFICAT ION

2.1. Use of Derivative Classification

2.1.1. Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. In the process of assigning a derivative classification, a derivative classifier will refer to original classification guidance (e.g., an NSA/CSS classification or declassification Guide, an OCA decision documented in an SPF) or a previously classified document that accurately reflects an OCA decision.

2.1.2. Derivative classifiers shall:

2.1.2.1. Be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

2.1.2.2. Observe and respect original classification decisions;

2.1.2.3. Carry forward to any newly created document the pertinent classification markings from the *source document(s)* or applicable classification guide(s);

2.1.2.4. Carry forward the date for declassification that corresponds to the longest period of classification among the sources; and

2.1.2.5. List the source documents.

2.1.3. See Annex A for additional guidance on marking.

2.1.4. Derivative classifiers shall, whenev er practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in an unclassified form.

2.2. Classification Guides

2.2.1. Agencies with original classification authority must prepare classification guides and declassification guides to facilitate the proper and uniform derivative classification of information. Information and guidance on creating NSA/CSS classification guides can be found in Annex B.

2.2.2. The absence of an item in a classification guide does not imply it is UNCLASSIFIED. If a holder of information believes the information should be classified but it is not covered by a classification guide, or a compilation of unclassified information should be classified, or information already classified should be classified at a higher level, the individual should handle and safeguard the information accordingly, tentatively mark the information along with the notation "pending classification review by [title of the appropriate OCA]," and contact the local classification advisory officer (CAO) and or Information Security Policy (DJ2) for further guidance.

3. SENSITIVE COMPARTMENTED INFORMATION

3.1. The term "Sensitive Compartmented Information" (SCI) refers to classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal control systems established by the Director of National Intelligence (DNI). The term "SCI control system" refers to the system of procedural protective mechanisms used to regulate or guide each program established by the DNI as SCI. A control system provides the ability to exercise restraint, direction, or influence over, or provide that degree of *access* control or physical protection necessary to regulate, handle, or manage information or items within an approved program. Within the SCI control systems are compartments and sub-compartments, each designed to formally segregate data and limit access to those with an absolute *need-to-know* as determined by a central authority for each compartment. Three SCI compartments most commonly used at NSA/CSS are:

3.1.1. Special Intelligence (SI) protects technical and intelligence information derived from the monitoring of foreign communications signals by other than the intended recipients. The SI control system protects SI-derived information and information relating to SI activities, capabilities, techniques, processes, and procedures [1];

3.1.2. HUMINT (Human Intelligence) Control System (HCS) protects the most sensitive HUMINT operations and information acquired from clandestine and/or uniquely sensitive HUMINT sources, methods, and certain technical collection capabilities, technologies, and methods linked to or supportive of HUMINT; and

3.1.3. TALENT KEYHOLE (TK) protects information and activities related to space-based collection of imagery, signals, measurement and signature intelligence, certain products, processing, and exploitation techniques, and the design, acquisition, and operation of reconnaissance satellites.

[1] The "COMINT" (i.e., *Communications Intelligence*) title for the SI control system is no longer valid. Any COMINT information formerly protected by now defunct COMINT marking or COMINT codewords is protected as SI.

4. DECLASSIFICATION AND DOWNGRADING

4.1. Authority for Declassification

4.1.1. Information shall be declassified as soon as it no longer meets the standards for classification (section 1.1). Decisions concerning the declassification or *downgrading* of information will be made by a declassification authority (generally, the OCA with purview over that information). When practicable , this will be the same OCA who originally classified the information, that OCA's successor, or a supervisor of the OCA or successor OCA – if that person has the authority to originally classify information , or by an official delegated declassification authority in writing by DIRNSA/CHCSS or by the Associate Director for Policy and Records (ADPR) (in the capacity of the Senior Agency Official).

4.1.2. The Director of National Intelligence may, in consultation with DIRNSA/CHCSS, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities relevant to NSA/CSS .

4.1.3. While it is presumed that classified information requires continued protection, in exceptional circumstances the need to protect such information may be outweighed by the public interest in disclosure of the information and should be declassified. The ADPR, in consultation with an OCA with purview over the information, shall make such a determination considering, among other factors, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

4.2. Declassification Programs

4.2.1. Declassification Services (DJ5) manages the automatic declassification program, the systematic declassification review progra m, and the mandatory declassification review (MDR) program for NSA/CSS.

4.2.1.1. Automatic Declassification :

4.2.1.1.1. All classified records that are more than 25 years old, have been determined to have permanent historical value under Title 44, United States Code, and have not been identified as exempt shall be automatically declassified, whether or not the records have been reviewed. All classified non-exempt records will be automatically declassified on 31 December of the year that is 25 years from the date of origin.

4.2.1.1.2. Exemptions from automatic declassification approved in accordance with E.O. 13526 (Reference b) may be incorporated into classification guides provided the Interagency Security Classification Appeals Panel (ISCAP) is notified in advance of the intent to take such action and the exempted information remains in active use.

4.2.1.2. Systematic Declassification Review: NSA/CSS conducts a program for systematic declassification review of records of permanent historical value exempted from automatic declassification .

4.2.1.3. MDR: Individuals may request an MDR of classified government records; see Policy 1-15, "Mandatory Declassification Review Program" (Reference k), for details.

4.2.2. NSA/CSS shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the Federal Records Act (Reference l).

5. CLASSIFICATION CHALLENGES

5.1. General Procedures

5.1.1. *Authorized holders* of information who, in good faith, believe that its classification status is improper (e.g., the information is marked unclassified but the holder believes it should be classified, or an item is marked TOP SECRET but the holder believes it should be CONFIDENTIAL) are encouraged and expected to challenge the classification status of the information.

5.1.2. No punitive action will be taken against an authorized holder who, in good faith, makes a classification challenge.

5.1.3. Information involved in a classification challenge shall continue to be protected at the level of its current classification level until a final decision is made on the challenge.

5.1.4. These procedures do not apply to documents that are required to be submitted for prepublication review (Reference m) or in an administrative process pursuant to an approved nondisclosure agreement.

5.1.5. NSA/CSS will not entertain classification challenges of information that has been the subject of a classification challenge within the past 2 years (to include information that has been the subject of a Freedom of Information Act or Privacy

Act (References g and j) request or mandatory declassification review request (Reference k) within the past 2 years), or that is the subject of pending litigation. Such requests will not be processed beyond informing the requester of this fact and of his/her appeal rights, if any.

5.2. Procedures for Submitting a Classification Challenge

5.2.1. Informal Classification Challenges: While not a required step in the classification challenge process, informal challenges to the classification status of a particular piece of information are encouraged. Such challenges may take any number of different forms, but the relevant classified information must at all times be handled and protected in a manner that accords with E.O. 13526 unless and until a final decision is made to declassify it. Informal questions may be directed to the originator/owner of the information and/or the local CAO. The list of NSA/CSS CAOs is available by typing *"go cao"* on NSANet.

5.2.2. Formal Classification Challenges: An authorized holder who wants to formally challenge the classification status of such information shall:

5.2.2.1. Present a challenge to the OCA with purview over the information and to the Office of Information Security Policy (DJ2) for tracking. The formal challenge must be in writing but need not be any more specific than to question why the information is or is not classified or why it is classified at a certain level. Upon receipt, the formal challenge shall be entered into the DJ2 system for processing, tracking, and recording formal classification challenges made by authorized holders.

5.2.2.2. The OCA with purview over the information shall review the challenge and provide an initial written response to a challenge within 60 days.

5.2.2.2.1. If the OCA is unable to review the challenge and respond within 60 days, the Agency must acknowledge the challenge in writing and provide the challenger with a date by which such a determination will be made. The acknowledgement shall also include a statement that, if no response is received within 120 days of the original notification, the challenger has the right to forward the challenge to the ISCAP for a decision.

5.2.2.2.2. If the OCA fails to provide an initial written response to a classification challenge within 120 days from the original notification, the challenger may forward the challenge to the ISCAP for a decision.

5.2.2.2.3. If the OCA issues an adverse determination of a classification challenge, the determination shall include notification that the

challenger has the right to submit an internal administrative appeal within 60 days of the date of the adverse determination to the ADPR.

5.2.2.3. The ADPR shall normally make a determination within 60 working days following the receipt of an appeal.

5.2.2.3.1. If additional time is required to make a determination, the ADPR shall notify the challenger of the additional time needed and provide the requester with the reason for the extension.

5.2.2.3.2. The ADPR shall notify the challenger in writing of the final determination, and, in the case of a denial, of the reason for the denial and of the challenger's final appeal rights to the ISCAP.

5.2.2.3.3. If the Agency fails to respond to the challenger within 90 days of the Agency's receipt of the appeal, the challenger may forward the challenge to the ISCAP.

6. SAFEGUARDING

6.1. An official or employee leaving Agency service may not remove classified information from the Agency's control or direct that information be declassified in order to remove it from Agency control.

6.2. Classified information may not be removed from official premises without proper authorization.

6.3. Persons authorized to disseminate classified information outside the Executive Branch shall ensure the protection of the information in a manner equivalent to that provided within the Executive Branch.

6.4. Consistent with this Guide and other relevant guidance, controls shall be established to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized individuals. In accordance with E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" (Reference n), this includes information sharing and safeguarding of classified information on computer networks.

6.5. NSA/CSS shall safeguard FGI under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. CONFIDENTIAL information, including modified handling and transmission and allowing

access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

6.6. Policy on special access programs can be found in NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information" (Reference o).

6.7. Individuals suspecting an unauthorized disclosure of NSA/CSS information should report it in accordance with NSA/CSS Policy 1-27, "Reporting Unauthorized Media Disclosures of Classified NSA/CSS Information" (Reference p), NSA/CSS Policy 5-5, "Reporting of Security Incidents and Criminal Violations" (Reference q), or NSA/CSS Policy 5-21, "Individual Security Reporting Requirements" (Reference r), as appropriate.

7. SELF-INSPECTION PROGRAM

7.1. Pursuant to E.O. 13526 (Reference b) and E.O. 13587 (Reference n), heads of agencies that originate or handle classified information are required to establish and maintain an ongoing self-inspection program that shall include the regular review and assessment of the Agency's Information Security Program. The purpose of a self-inspection is to review and assess an organization's classified product and its procedures for protecting that product.

7.2. The Senior Agency Official directs and administers the Agency's self-inspection program through the Office of Information Security Policy (DJ2) and CAOs Agency-wide. The program provides the Senior Agency Official with information necessary to assess the effectiveness of the classified national security information program within individual activities and in the Agency as a whole (Reference c). Self-inspections evaluate adherence to References b and c and the effectiveness of Agency programs addressing original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

7.3. The self-inspection of an NSA/CSS element consists of three parts:

7.3.1. Review of a random sampling of classified materials (e.g., email, reports, presentations and webpages) to gauge organizational proficiency in marking mechanics;

7.3.2. Interviews of organization personnel to assess typical attitudes and awareness relative to classification policy and information handling issues; and

7.3.3. Information Security program discussions with the organizational CAO to document additional issues, review a sampling of CAO correspondence, and provide recommendations and resources that could lead to a stronger program.

7.4. For additional information on items that will be addressed during self-inspections, see the "NSA/CSS Information Security and Self-Inspection Program Evaluation" and the

"NSA/CSS Information Security Self-Inspection Program Standard Operating Procedures" (Reference s).

8. REFERENCES

a. NSA/CSS Policy 1-52, "Classified National Security Information," dated 16 November 2012.

b. Executive Order 13526, "Classified National Security Information," dated 5 January 2010.

c. Information Security Oversight Office Implementing Directive for E.O. 13526, 32 CFR Parts 2001 and 2003, dated 28 June 2010.

d. ICD 710, "Classification Management and Control Markings System," dated 21 June 2013.

e. Controlled Access Program Coordination Office (CAPCO) Intelligence Community Authorized Classification and Control Markings Register and Manual, Version 6, Edition 1 (Version 5.1), dated 28 February 2013.

f. DoDM 5200.01 Volume 2, "DoD Information Security Program: Marking of Classified Information," dated 24 February 2012.

g. United States Code Section 552, Freedom of Information Act.

h. NSA/CSS Policy 1-5, "NSA/CSS Freedom of Information Act Program," dated 24 May 2004.

i. Presidential Records Act of 1978, Title 44, United States Code, Sections 2201 – 2207, as amended.

j. Title 5, United States Code Section 552a, Privacy Act, dated 7 July 2004.

k. NSA/CSS Policy 1-15, "Mandatory Declassification Review Program," dated 13 June 2013.

l. Federal Records Act of 1950.

m. NSA/CSS Policy 1-30, "Review of NSA/CSS Information for Public Release," dated 10 May 2013.

n. Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," dated 7 October 2011.

o. NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information," dated 7 March 2013.

p. NSA/CSS Policy 1-27, "Reporting Unauthorized Media Disclosures of Classified NSA/CSS Information," dated 20 March 2006.

q. NSA/CSS Policy 5-5, "Reporting of Security Incidents and Criminal Violations," dated 3 August 2010.

r. NSA/CSS Policy 5-21, "Individual Security Reporting Requirements," dated 3 May 2012.

s. NSA/CSS Information Security Self-Inspection Program Evaluation: Standard Operating Procedures dated June 2013.

t. Executive Order 12333, "United States Intelligence Activities," as amended.

u. ICD 403, "Foreign Disclosure and Release of Classified National Intelligence," dated 13 March 2013.

v. DCID 6/7, "Intelligence Disclosure Policy."

w. National Disclosure Policy (NDP-1).

x. ICPG 710.1, "Application of Dissemination Controls: Originator Control," dated 25 July 2012.

y. ODNI National Counterintelligence Executive (NCIX 260-11), "DNI Guidance for Intelligence Community Marking Challenge Procedures," dated 18 January 2012.

z. DoDM 5200.45, "Instructions for Developing Security Classification Guides," dated 2 April 2013.

aa. "NSA/CSS Declassification Guide" dated 14 September 2012.

9. DEFINITIONS

9.1. Access – The ability or opportunity to gain knowledge of classified information (Reference b).

9.2. Authorized holder – A person who may have access to classified information provided that:

9.2.1. A favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

9.2.2. The person has signed an approved nondisclosure agreement; and

9.2.3. The person has a need-to-know the information.

9.3. Automatic declassification – the declassification of information based solely upon:

9.3.1. The occurrence of a specific date or event as determined by the OCA; or

9.3.2. The expiration of a maximum timeframe for duration of classification established under E.O. 13526 (Reference b).

9.4. Classification – The act or process by which information is determined to be classified information (Reference b).

9.5. Classification guide – A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element (Reference b).

9.6. Classified national security information – Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

9.7. Classify – See classification.

9.8. Damage to national security – Harm to the national defense or foreign relations of the U.S. from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, or provenance of that information.

9.9. Declassification – The authorized change in the status of information from classified information to unclassified information (Reference b).

9.10. Declassification guide – Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified (Reference b).

9.11. Declassify – See declassification.

9.12. Derivative classification – Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

9.13. Downgrading – A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

9.14. Foreign government information – (1) Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence; (2) information produced by the U.S. Govenment pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence; or (3) information received and treated as "foreign government information" under the terms of a predecessor order.

9.15. Intelligence – Foreign intelligence and counter intelligence as defined in E.O. 12333 (Reference t).

9.16. Intelligence activities – All activities that elements of the Intelligence Community are authorized to conduct pursuant to E.O. 12333 (Reference t).

9.17. Mark – See marking.

9.18. Marking – To identify the classification of information (Reference f).

9.19. Multiple sources – Two or more source documents, classification guides, or a combination of both.

9.20. Need-to-know – A determination within the Executive Branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful or authorized governmental function.

9.21. Original classification – An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

9.22. Original classification authority (OCA) – An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

9.23. Safeguarding – Measures and controls that are prescribed to protect classified information.

9.24. Senior agency official – The official designated by the agency head to direct and administer the agency's program under which information is classified, safeguarded, and declassified. At NSA/CSS this is the Associate Director for Policy and Records.

9.25. Source document – An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

ANNEX A

MARKING GUIDANCE

1. General

1.1. E.O. 13526 (Reference b) prescribes a uniform system for classifying, safeguarding, and declassifying national security information while allowing public access when possible. This uniform system requires that standard markings be applied to classified and declassified information, and markings not deviate from prescribed formats. The Office of the Director of National Intelligence and the Department of Defense provide consistent standards for a uniform list of authorized classification and control markings and their authorized abbreviations and portion markings pursuant to E.O. 13526 and Information Security Oversight Office (ISOO) Implementing Directive (References b and c).

1.2. IC authorized classification and control marking guidance is provided in the Controlled Access Program Coordination Office (CAPCO) Register and Manual (Reference e). DoD guidance for marking classified military information is contained in DoD Manual 5200.01, Volume 2 (Reference f). This Annex provides marking guidance common to both DNI and DoD. See Appendix 1 for marking guidance unique to DNI. See Appendix 2 for information unique to DoD.

1.3. Marking guidance in this manual is applicable to all information under the purview of the United States Cryptologic System (USCS); however, it cannot describe every possible situation that might arise and there will be times when this guidance will need to be applied in a flexible manner. At times when no marking guidance exists, the spirit of E.O. 13526 and the ISOO Implementing Directive (References b and c) shall be followed in a manner that best safeguards the information.

1.4. If classification and control markings cannot be affixed to specific classified information or materials, the OCA shall provide written instructions for protecting the information. Similarly, if declassification markings cannot be affixed to specific information or materials, the OCA shall provide holders or recipients of the information with written instructions for marking the information.

2. Original Classification

2.1. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

2.2. At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

2.2.1. Classification Authority: the name and position, or personal identifier, of the original classification authority (OCA) shall appear on the "Classified By" line. If not otherwise evident, the agency and office of origin shall be identified and follow the name of the OCA.

2.2.2. Reason for classification: the OCA shall identify the reason(s) for the decision to classify on the "Reason" line. Include on this line the number 1.4 plus the letter(s) that corresponds to that classification category in paragraph 1.1.1.3 of this policy.

2.2.3. Declassification instructions: The duration of the original classification decision shall be placed on the "Declassify On" line. When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD. Events shall be reasonably definite and foreseeable, such as Completion of Operation. The OCA will apply a duration consistent with section 1.4.1 of this policy.

2.2.4. An example of an original classification block might appear as:

Classified By: dwsmith, Chief, Support Services
Reason: 1.4(d)
Declassify On: 20350530
or

Classified By: David W. Smith, Chief, Support Services
Reason: 1.4(d)
Declassify On: Completion of project.

2.2.5. The date of origin of the document.

3. Derivative Classification

3.1. Derivative classification markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

3.2. A classification authority block must be clearly identified and include the following:

3.2.1. "Classified By" line indicating the individual doing the derivative classification. Either the individual's SID or employee identification number may be used;

3.2.2. "Derived From" line indicating the source of the classification determination;

3.2.3. "Dated" line indicating, in YYYYMMDD format, the date of the source document or classification guide in the "Derived From" line; and

3.2.4. "Declassify On" line indicating the declassification instructions for the document. For most NSA/CSS information the declassification date is 25 years from the date a document is created. If the declassification instruction is a date, the format is YYYYMMDD.

3.3. Derivative classifiers shall be identified by name and position, or by personal identifier, in a matter that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin shall be identified and follow the name on the "Classified By" line. An example might appear as

Classified By: Peggy G. Jones, Lead Analyst or

Classified By: pgjones

3.4. The derivative classifier shall concisely identify the source document or the classification guide on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as

Derived From: Memo, "SUGARHONEY Preparations," NSA/CSS, SID
or
Derived From: NSA/CSS SUGARHONEY Classification Guide
or
Derived From: NSA/CSSM 1-52

3.5. When a document is classified derivatively on the basis of more than one source document or classification guide, the derivative classifier shall include a listing of the source materials on, or attached to, each derivatively classified document and the "Derived From" line shall appear as:

Derived From: *Multiple Sources*

3.6. The derivative classifier shall carry forward the "Declassify On" line from the source document to the derivative document, or the duration instruction from the classification or declassification guide. If the source document is missing the declassification instruction, then a calculated date of 25 years from the date of the source document or the current date (if the source document date is not available) shall be carried forward by the derivative classifier.

3.7. When a document is classified derivatively on the basis of multiple documents, the "Declassify On" line shall reflect the longest duration of any of its sources. When a document is classified derivatively either from a source document or classification guide that contains either declassification instructions Originating Agency's Determination Required, "OADR," Manual Review, "MR," or any of the exemption markings (i.e., X1, X2, etc.), the derivative classifier shall calculate a date that is 25 years from the date of the

source document when determining a derivative document's date to be placed in the "Declassify On" line.

3.8. Sample classification authority block:

Classified By: pgjones
Derived From: NSA/CSS SUGARHONEY Classification Guide
Dated: 20100529
Declassify On: 20350529

4. Primary Markings

4.1. Overall marking. The highest level of classification is determined by the highest level of any one portion within the document. Place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). The overall classification and control marking string is referred to as the "banner line."

4.1.1. For documents containing information classified at more than one level, the banner line shall be the aggregate of the highest level of classification and the most restrictive control marking(s). For example, if a document contains some information marked "SECRET//NOFORN" and other information marked CONFIDENTIAL//SI//REL TO USA, FVEY," the banner line would be "SECRET//SI//NOFORN."

4.1.2. Each interior page of a classified document shall be marked at the top and bottom with either the highest overall classification of the information on that page or the highest overall classification of the document, preferably the latter.

4.2. Portion Marking. Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, signature blocks, bullets, and other portions within slide presentations shall be marked to indicate which portions are classified and which portions are unclassified by placing a parenthetical symbol immediately preceding the portion to which it applies. Each portion marking shall indicate the highest classification level and control of information contained within the specific portion. Portion marking is not required if a document comprises completely unclassified information. However, if a single portion is classified or contains controlled unclassified information (e.g., U//FOUO), then the entire document must be portion marked. References e and f provide detailed guidance on portion marking.

4.2.1. To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, and "(C)" for Confidential will be used. Portions that do not meet the standards for classification shall be marked with "(U)" for Unclassified or "(U//FOUO)" for Unclassified//For Official Use Only to indicate controlled unclassified information.

4.2.2. In cases where portions are segmented such as paragraphs, sub-paragraphs, bullets, or sub-bullets, and the classification level is the same throughout, it is sufficient to put only one portion marking at the beginning of the main paragraph or main bullet. If there are different levels of classification among these segments, then all segments shall be portion marked separately in order to avoid over-classification of any one segment.

4.2.3. If the information contained in a sub-paragraph or sub-bullet is a higher level of classification than its parent paragraph or parent bullet, this does not make the parent paragraph or parent bullet classified at the same level. Each portion shall reflect the classification level of that individual portion and not any other portions.

4.2.4. Uniform Resource Locators (URLs) shall be portion marked based on the classification of the content of the URL itself. The URL shall not be portion marked to reflect the classification of the content to which it points. For clarity, a notice may be included after a link to indicate that it will take the reader to a classified document, for example:

(U) Link to Final Report (Report is TOP SECRET)

or

http://www.proj.nsa.ic.gov/cente_rdub_(TS).html

4.2.5. Portion markings shall include any control markings applicable to the portion.

4.3. Control Markings. Control markings are used in the overall classification line and portion marking to identify control systems that provide additional access control or physical protection for the information or items covered by the program (e.g., SCI) or to identify the expansion or limitation on the distribution of information (i.e., dissemination controls). These markings are in addition to and separate from the levels of classification (e.g., TOP SECRET, SECRET, CONFIDENTIAL). See Appendix A-1 and Appendix A-2 for additional guidance.

4.4. Within the portion marking and banner line, double forward slashes (//) separate the classification and control markings and also separate the categories of control markings. Single forward slashes (/) separate multiple control markings within the same category. Hyphens (-) are used to separate control markings and their sub-controls (see Figure 1).

Figure 1: Examples of markings
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Banner Line	Portion Marking
TOP SECRET//SI/TK//REL TO USA, AUS	(TS//SI/TK//REL)
SECRET//SI/TK//RELIDO	(S//SI/TK//RELIDO)
TOP SECRET//SI-GAMMA//ORCON/NOFORN	(TS//SI-G//OC/NF)
CONFIDENTIAL //REL TO USA, FVEY	(C//REL TO USA, FVEY)
UNCLASSIFIED//FOR OFFICIAL USE ONLY	(U//FOUO)

5. Transmittal Documents

5.1. Transmittal documents are documents that have information enclosed with or attached to them. An example is a letter, memorandum, or summary sheet with enclosures. The transmittal document itself may or may not be classified and may or may not contain classified information.

5.2. If the transmittal document does not contain classified information, mark the banner line at the top and bottom of each page with the highest classification level of any information being transmitted. Also mark the transmittal document with an appropriate instruction such as placing the following on the face of the document:

"Upon removal of attachment(s) this document is UNCLASSIFIED."

5.3. If the transmittal document itself contains classified information, mark it as required for all other classified information, including portion markings, classification authority block, and the full text, and:

5.3.1. Mark the banner line of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures.

5.3.2. Mark the transmittal document with the appropriate instruction indicating its overall classification level if the level will change when the enclosures are removed (e.g., "Downgrade to CONFIDENTIAL when separated from SECRET enclosures").

5.4. When an electronic document contains a file attachment or other embedded information, that document is considered a transmittal document for classification purposes. The overall

classification markings for the electronic document should reflect the most restrictive markings of all embedded information.

5.5. Additional classification marking guidance for NSA/CSS material may be found by typing *"go class-mark"* on NSANet.

6. Classification marking in the electronic environment

6.1. Classified national security information in the electronic environment shall be 1) subject to all requirements of E.O. 13526 (Reference b); 2) marked with proper classification markings to the extent that such marking is practical; 3) marked with proper classification markings when appearing in an electronic output (e.g., database query); 4) marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the OCA; and 5) prohibited from use as the source of the derivative classification if it is dynamic in nature (e.g., wikis and blogs) and where information is not marked in accordance with Reference b.

6.2. Marking classified email messages.

6.2.1. Classified email messages transmitted on or prepared for transmission on NSANet must display the overall classification at the top and bottom of the body of each message. The overall classification and control marking string for the email shall reflect the classification of the header and body of the message, including the subject line, the text of the email, the signature block, any attachments, any included message(s), and any other information that is conveyed in the email. The overall classification and control marking string shall follow the format:

CLASSIFICATION: [*classification and control marking string*]

6.2.2. Subject lines shall be portion marked to reflect the sensitivity of the information in the subject line.

6.2.3. Classified email shall be portion marked to reflect the highest level of information contained in that portion.

6.2.4. The signature block shall be portion marked to reflect the highest classification level and control of the information contained in the signature block itself.

6.2.5. When forwarding or replying to an email, ensure required markings reflect the overall classification and control markings and classification authority block for the entire string of emails and attachments, including any newly drafted material received from previous senders and any attachments.

6.3. Marking webpages with classified content.

6.3.1. Webpages shall be classified and marked on their own content regardless of the classification of the pages to which they link. In general, the following guidelines apply:

6.3.1.1. The banner line for every webpage shall reflect the overall classification and control marking(s) for the information on that page. Linear text entered at the top and bottom of the page is acceptable. A set of colored classification bars approved by the Office of Policy and Records (DJ) is available ("*go image*," then click on the "class/" link).

6.3.1.2. Webpages containing no classified content shall include banners marked UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY, as appropriate.

6.3.1.3. All content on classified webpages shall be portion marked, to include any point of contact (POC) information present on the page. Additionally, these webpages shall include the classification authority block at the bottom of the page.

6.3.1.4. Electronic media files (e.g., video, audio, images, or slides) shall carry overall classification and the classification authority block unless the addition of such information would render them inoperable.

6.3.2. A dynamic page contains information derived from a changeable source or ad hoc query, such as a database. The classification and control marking(s) for the information returned may vary depending on the specific request.

6.3.2.1. If there is a mechanism for determining the actual classification and control marking(s) for each response, then those shall be displayed in the response. If such a mechanism does not exist, then the following marking shall be used:

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS [insert classification]

6.3.2.2. The dynamic page marking shall appear on a webpage above the primary classification and control marking string with the highest possible overall classification and control marking(s) for information that can be retrieved. For example:

DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

6.3.2.3. The combination of the dynamic marking and the classification and control marking string informs the viewer of the highest level of information that may appear, although the classification and control marking(s) for any particular information retrieved may be lower. This banner can be found with other approved classification banners ("*go image*," then click on the "class/" link).

6.3.3. Classified Blogs and Wikis

6.3.3.1. The overall classification and control marking string for blog entries or wiki articles shall reflect the overall classification markings for the highest level of information allowed in that space. While the content of an overall blog is dynamic, entries are generally static in nature. Blog entries or comments and wiki articles or submissions shall be portion marked to reflect the highest level of information contained in that portion, not the content of the post.

6.3.4. Controlled Imports

6.3.4.1. Users may see unclassified pages that have been authorized for import from an external source (such as the Internet or a CD-ROM). Such pages shall carry the marking:

UNCLASSIFIED – CONTROLLED IMPORT FROM AN EXTERNAL SOURCE

6.3.4.2. This marking was created to identify information that is unclassified when imported from an external source but might be protected if associated with NSA/CSS. This banner can be found with other approved classification banners ("*go image*," then click on the "class/" link).

6.3.4.3. Completely UNCLASSIFIED imported documents in a format that does not allow for editing (e.g., PDF) may be hosted on NSANet in their native form without the otherwise-required banner.

6.4. Classified computer media such as USB sticks, hard drives, CD ROMs, and diskettes shall be marked to indicate the highest overall classification of the information contained within the media.

7. Markings on declassified information

7.1. Declassification markings shall be uniformly and conspicuously applied to information to leave no doubt about the declassified status of the information and who authorized the declassification.

7.2. Apply the following markings to records, or copies of records, regardless of media:

7.2.1. The word "Declassified;"

7.2.2. The identity of the declassification authority, by name and position, or by personal identifier, or the title and date of the declassification guide. If the identity of the declassification authority must be protected, a personal identifier may be used or the information may be retained in Agency files;

7.2.3. The date of declassification; and

7.2.4. The overall classification markings that appear on the cover page or first page shall be lined with an "X" or straight line. An example might appear as:

~~SECRET~~
Declassified by David Smith, NSA/CSS Chief Information Officer
on August 17, 2008

8. Marking Compilations

8.1. When marking materials for which the compilation principle applies, portions shall be marked to reflect only the information contained within that portion. The overall classification and control marking string shall reflect the highest classification and most restrictive control marking(s) applicable to the information revealed by the compilation of information.

8.2. A clear explanation for the classification as a result of compilation shall be provided to explain the relationship between the portion marking(s) and the overall classification and control marking string. The explanation shall be portion marked as needed and placed at the bottom of the first page of the document or the end of a soft copy file, for example:

(U) "This document is classified [*fill in classification and control marking(s)*] due to the compilation of information."

APPENDIX 1 TO ANNEX A

IC CLASSIFICATION AND CONTROL MARKINGS

1. The DNI maintains oversight of the 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 (See Reference d).

2. In accordance with DNI policies, a classification and control 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. The proper application and use of classification and control markings enables information sharing while allowing the information to be properly safeguarded from inadvertent or unauthorized disclosure. The IC classification and control markings system is implemented and maintained through the CAPCO Register and Manual (Reference e).

3. Foreign Disclosure Release Markings

3.1. NOFORN is an explicit foreign release marking used to indicate the information may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator and in accordance with provisions of the CAPCO Register and Manual (Reference e), ICD 403, "Foreign Disclosure and Release of Classified National Intelligence" (Reference u), DCID 6/7, "Intelligence Disclosure Policy," and NDP-1 (References v - w).

3.2. REL TO is an explicit foreign release marking used to indicate the information has been predetermined by the originator to be releasable or has been released to the foreign country(ies)/international organization(s) indicated, through established foreign disclosure procedures and channels, and implementation guidance in Reference e. It is NOFORN to all other foreign country(ies)/international organization(s) not indicated in the REL TO marking. Per ICD 403 (Reference u), release is defined as the provision of classified intelligence, in writing or in any other medium, to authorized foreign recipients for retention. See Reference e for detailed guidance on the use of the REL TO marking.

3.3. RELIDO is a permissive foreign release marking used on information to indicate that the originator has authorized a Senior Foreign Disclosure and Release Authority (SFDRA) to make further sharing decisions for uncaveated intelligence material (intelligence with no restrictive dissemination controls) in accordance with the existing procedures, guidelines, and implementation guidance in Reference e.

3.4. DISPLAY ONLY is used to indicate the information is authorized for disclosure without providing the foreign recipient with a physical copy for retention, regardless of medium to the foreign country(ies)/international organization(s) indicated, through established foreign

disclosure procedures and channels, and implementation guidance in Reference e. Per ICD 403 (Reference u), disclosure is defined as displaying or revealing classified intelligence whether orally, in writing, or in any other medium to an authorized foreign recipient without providing the foreign recipient a copy of such information for retention.

4. To facilitate the appropriate foreign disclosure and release of intelligence information, the following applies:

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

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

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

4.3.1. 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

4.3.2. 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;

4.4. 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

4.5. Foreign disclosure or release decisions shall be consistent with ICD 403 (Reference u).

5. NSA/CSS 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 be duplicative of any markings in the CAPCO Register and Manual (Reference e). NSA/CSS specific internal controls shall not be used when information is disseminated outside the Agency.

6. NSA/CSS may apply caveats or warnings to communicate distribution or handling instructions for 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.

7. Controls on the dissemination and use of classified national intelligence are necessary to protect intelligence sources, methods, and activities. Use of the originator control (ORCON) dissemination control marking 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 to ensure that classified national intelligence is disseminated appropriately without undue delay or restriction. ICPG 710.1 (Reference x) provides direction and guidance for the application and use of the originator control (ORCON) dissemination control marking.

8. Control Marking Challenges

8.1. NSA/CSS control marking challenge procedures are established in accordance with ICD 710 and DNI Guidance for Intelligence Community Marking Challenges (NCIX 260-11) (References d and y). Authorized holders of information who, in good faith, believe that its control marking is improper (e.g., the banner is marked SECRET//SI/TK//NOFORN but the holder believes it should be marked SECRET//SI//NOFORN) are encouraged and expected to challenge the control marking status of the information.

8.2. No punitive action will be taken against an authorized holder who, in good faith, makes a control marking challenge.

8.3. Information involved in a control marking challenge shall continue to be protected at the level of its current classification level until a final decision is made on the challenge.

8.4. Procedures for a Control Marking Challenge

8.4.1. Informal Control Marking Challenges.

8.4.1.1. Authorized holders of information may first seek resolution of a control marking challenge with the originator of the information.

8.4.1.2. If the originator cannot be determined or is unavailable, of if the challenger is not satisfied with the originator's response, challengers shall contact the originator's local CAO to request a review. While the CAO cannot overturn an OCA decision, the CAO may assist in deciding whether it is advisable to further pursue a challenge. The list of NSA/CSS CAOs is available by typing *"go cao"* on NSANet.

8.4.1.3. If the CAO's assistance does not resolve the challenger's concern, the originator or the CAO shall contact the Classification Review Team in the Office of Information Security Policy (DJ2) (dl class review) for a determination.

8.4.1.4. If the matter is not resolved, the challenger may submit a formal challenge in writing to the ADPR.

8.4.2. Formal Control Marking Challenges. In addition to the guidelines above, formal control marking challenge procedures include:

8.4.2.1. The authorized holder shall present the challenge, in writing, to the ADPR. The formal challenge need not be any more specific than to question the control marking and provide a rationale.

8.4.2.2. The ADPR shall provide an initial written response to a challenge within 60 days.

8.4.2.3. If the ADPR is unable to review the challenge and respond within 60 days, the Agency must acknowledge the challenge in writing and provide the challenger with a date by which such a determination will be made. The acknowledgement shall also include a statement that, if no response is received within 120 days from the original notification, the challenger has the right to forward the challenge, in writing, to the Office of the National Counterintelligence Executive Special Security Directorate (ONCIX/SSD) for a decision.

8.4.2.4. If the ADPR issues an adverse determination of a control marking challenge, the determination shall include notification that the challenger has the right to submit an appeal, in writing, to the ONCIX/SSD.

8.5. Control Marking Challenge Appeals: Authorized holders of information who continue to question the formal control marking challenge determination may submit an appeal to the ONCIX/SSD in accordance with NCIX-260-11 (Reference y).

9. **Portion Marking Waivers.**

9.1. In accordance with References c, e, and f, only the Director of the ISOO may grant waivers to marking requirements specified by E.O. 13526 (Reference b) for classified information. Approved portion marking waivers will be temporary and will have specific expiration dates.

9.2. Any NSA/CSS marking waiver request, including portion marking waiver requests, must be submitted by the Senior Agency Official (i.e., ADPR) to the CAPCO, for forwarding to the Director, ISOO. Notices of approved portion marking waivers are maintained by the Office of Policy and Records (DJ).

9.3. A waiver request shall include the reasons that the benefits of portion marking are outweighed by other factors, and the request must also demonstrate that the requested waiver will not create impediments to information sharing.

9.4. A document not portion marked based on an ISOO-approved waiver must:

9.4.1. Not be used as a source for derivative classification, nor can it be used as a source for preparers of classification guides.

9.4.2. Contain a caveat that states, "WARNING: THIS DOCUMENT CANNOT BE USED AS A SOURCE OF DERIVATIVE CLASSIFICATION."

9.4.3. Be portion marked when transmitted or disseminated outside the NSA/CSS, unless the ISOO waiver approval explicitly provides otherwise.

APPENDIX 2 TO ANNEX A

DOD CLASSIFICATION AND CONTROL MARKINGS

1. The DoD maintains oversight of the DoD Information Security Program, which provides procedures for the designation, marking, protection, and dissemination of controlled unclassified information and classified military information. The proper application and use of DoD classification and control markings enables the identification and protection of national security information and promotes information sharing.

2. Classified military information falls under the purview of DoD. Per the National Disclosure Policy (NDP-1) (Reference w), classified military information is military information requiring protection in the interest of national security and is limited to three classifications: TOP SECRET, SECRET, and CONFIDENTIAL. Classified military information is further subdivided into eight categories:

    a. Organization, Training and Employment of Military Forces
    b. Military Materiel and Munitions
    c. Applied Research and Development Information and Materiel
    d. Production Information
    e. Combined Military Operations, Planning and Readiness
    f. U.S. Order of Battle
    g. North American Defense
    h. Military Intelligence

3. **Foreign Disclosure Release Markings**

3.1 Authorized for Release To (REL TO):

3.1.1 The AUTHORIZED TO RELEASE TO or REL TO control marking is authorized for use on all classified military information that has been determined by an authorized disclosure official to be releasable, or that has been released through established foreign disclosure procedures and channels, to the foreign country and/or international organization indicated.

3.1.2 For documents containing REL TO portions, if the document is not fully releasable to at least one country other than U.S. or an international organization, the banner line shall not contain the REL TO marking.

3.2 Not Releasable to Foreign Nationals (NOFORN): NOFORN shall not be applied to non-intelligence information, except for Naval Nuclear Propulsion Information and NDP-1 (Reference w), which have authorized exceptions for use of NOFORN. In all other instances, within the DoD NOFORN shall be used only on intelligence information.

4. Detailed guidance for the marking of classified military information is contained in DoDM 5200.01, Volume 2 (Reference f).

5. Instructions for developing security classification guides can be found in DoDM 5200.45 (Reference z).

ANNEX B

DOCUMENTING ORIGINAL CLASSIFICATION DECISIONS

1. E.O. 13526 (Reference b) mandates all agencies with original classification authority prepare classification guides to facilitate the proper and uniform derivative classification of information. A classification guide is required for every topic (e.g., a system, plan, program, project, operation, or equipment) under the purview of NSA/CSS that is classified. Classification guides document original classification decisions and must be approved by an OCA with purview over the information. Classification guides may also include items that are determined to be unclassified or controlled unclassified information.

2. A declassification guide documents both the elements of information on a specific subject that may be declassified and the elements that must remain classified. Declassification guides must also be approved in writing by an OCA with purview over the information. The "NSA/CSS Declassification Guide" (Reference aa) provides guidance on NSA/CSS information that may remain classified after 25 years.

3. An Information Management Instruction (IMI), which is unique to NSA/CSS and is similar to a classification guide, documents decisions that are either all UNCLASSIFIED or UNCLASSIFIED//FOR OFFICIAL USE ONLY. Like classification and declassification guides, IMIs are approved in writing by an OCA with purview over the information.

4 Classification guides, declassification guides, and IMIs are categorized based on the type of information they describe, consistent with the NSA/CSS corporate policy structure:

(U) Series 01 – Corporate, Management, Governance
(U) Series 02 – SIGINT
(U) Series 03 – Information Assurance
(U) Series 04 – Human Resources
(U) Series 05 – Security
(U) Series 06 – Information Technology
(U) Series 07 – Finance
(U) Series 08 – Acquisition
(U) Series 09 – Installations and Logistics
(U) Series 10 – Miscellaneous
(U) Series 11 – Mission Integration and Cyber

5. NSA/CSS classification guides, declassification guides, and IMIs, unless special access is required, will be maintained on NSANet ("*go classguides*") and selected ones are also available on Intelink at http://www.nsa.ic.gov/produce r/refs/classguide/ and on SIPRNet at http://nsaintelinks.intelink.sgo v.gov/producer/refs/classguideSi pr.

6. NSA/CSS topic-specific classification documents are functionally considered appendices to this overarching Guide, and formal statements of NSA/CSS classification policy. For this reason, the most common derivative classification information at NSA/CSS states that the information being derivatively classified is derived from NSA/CSSM 1-52. This Guide and its associated classification guides, declassification guides, and IMIs are to be used for derivative classification by all NSA/CSS employees generating classified NSA/CSS information.

7. This Guide and its associated classification guides, declassification guides, and IMIs pertain only to information under the purview of the USCS. The guidance herein cannot be used to classify information that belongs to other IC or DoD elements. Derivative classifiers should follow the classification guidance of the pertinent IC agency or DoD component when considering the proper handling or classification levels of that information.

8. A classification guide must be reissued, cancelled, or certified current within 5 years of its publication. If not, the guide will expire effective 10 years from its issue date and will be removed from the NSA/CSS classification guide webpages on NSANet, Intelink, and SIPRNet.

9. Changes to classification guides, declassification guides, and IMIs will be incorporated as necessary to keep them current and relevant through the use of a change register. Users are encouraged to assist in improving and maintaining NSA/CSS classification guidance. Requests for changes should be forwarded through appropriate organizational staff levels to Information Security Policy/DJ2. Information Security Policy/DJ2 is responsible for maintaining classification guidance in conjunction with a specific guide's information owner. Requests for change will receive official vetting through all stakeholders. Program managers should be aware that the information that needs protection may change as a system, plan, program, project, or mission progresses through its life cycle. What needs to be classified in the early stages of a system, plan, program, project, or mission (e.g., during research and development) may differ from that which requires classification in other life-cycle phases (e.g., system development, production, operations, or execution). The classification guidance must be regularly reevaluated to determine updates as appropriate.

10. Portions of the classification guides, declassification guides, and IMIs may be extracted or reproduced by authorized users for local use. Users must strictly adhere to all classification and handling restrictions when storing hard- or soft-copies of NSA/CSS guides or when hyperlinking to NSA/CSS guides. However, such reproductions are unofficial documents and over time may no longer reflect the most current guidance. Derivative classifiers are responsible for ensuring that they are basing their decisions on the most current classification guidance. See guidance on NSANet ("*go classguides*"), Intelink, or SIPRNet.

11. NSA/CSS classification guides, declassification guides, and IMIs are not releasable to any Third Party partner without prior approval from the Chief, Information Security Policy (DJ2).

12. USCS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the NSA/CSS Extended Enterprise are pre-authorized for access to NSA/CSS classification guides, declassification guides, and IMIs via NSANet, JWICS, SIPRNet, or in hard-copy formats as needed to perform their jobs. Non-USCS contractors or consultants working at external facilities are pre-authorized for soft-copy access to NSA/CSS classification guidance via NSANet, JWICS or SIPRNet, if connectivity to those systems is allowed by the contractor's sponsor. Where such connectivity is not established, any hard-copy provision of NSA/CSS classification guidance must be authorized by the Chief, Information Security Policy (DJ2).

13. Further dissemination of NSA/CSS classification guides, declassification guides, and IMIs, to include posting on networks other than NSANet, JWICS or SIPRNet, is not authorized without prior approval from the Chief, Information Security Policy (DJ2).

14. Further information on creating classification guides and IMIs can be found on the DJ2 Developing Classification Guide webpage by typing *"go develop-class-guides"* on NSANet.