January 22, 2013

Inspector General
United States Department of Defense

A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the "Reducing Over-Classification Act"

Council of the Inspectors General on Integrity and Efficiency

This guide was prepared on behalf of the Council of the Inspectors General on Integrity and Efficiency

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

Preface

At the request of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Inspection and Evaluation Committee and with the approval of the CIGIE Executive Council, the Department of Defense Office of Inspector General (OIG) was asked to lead efforts to develop a common framework for conducting evaluations under Public Law 111-258, the "Reducing Over-Classification Act." A working group was established, consisting of the following OIGs: Intelligence Community, National Security Agency, National Reconnaissance Office, Defense Intelligence Agency, National Geospatial-Intelligence Agency, Environmental Protection Agency, Nuclear Regulatory Commission, and the Departments of State, Homeland Security, Justice, Energy, the Treasury, Transportation, Health and Human Services, and Agriculture. In consultation with representatives from the Information Security Oversight Office, this collaborative effort led to issuing this evaluation guide for OIG use when conducting evaluations.

The National Commission on Terrorist Acts Upon the United States (commonly known as the "9/11 Commission") observed that the "over-classification of information interferes with accurate, actionable, and timely information sharing, increases the cost of information security, and needlessly limits stakeholders and public access to information." Information is even more valuable when shared with those who need it. Yet, certain information must be held in confidence to protect our national security. These conflicting concerns require careful balancing between requirements to safeguard national security information and a responsibility to share it with other government officials who need to know the information to do their jobs. Only through the accurate and accountable application of classification standards, and dissemination control and handling markings (which are in addition to, and separate from, the level of classification, but identify the expansion or limitation on the distribution of the information) can we begin to constrain over-classification.

This evaluation guide provides detailed guidance for OIGs to use in evaluating their agencies' processes and follows the tenets outlined in Executive Order 13526, "Classified National Security Information," and its implementing directive, 32 Code of Federal Regulations, Part 2001, "Classified National Security Information." It is meant to serve as a guide, and not to be all encompassing, in order to allow for the unique requirements of each agency while maintaining a standard framework. We want to express our deep appreciation to all who contributed to the preparation of this guide.

Lynne M. Halbrooks
Principal Deputy

Table of Contents

I. General Information

A. Introduction

Key enablers of effective information sharing are strong classification management and control markings systems. Critical components of such systems are: (1) establishing a common understanding of the information that needs to be protected, why it needs protection, how long the information must remain classified; (2) the standards and procedures for communicating and marking the classification level and dissemination controls; and (3) strong program oversight. To assess the application of classification management and dissemination control marking standards, the [organization] will conduct an evaluation of classification management and control marking systems of classified national security information (CNSI) in accordance with P.L. 111-258. This document is guidance for OIGs to use in evaluating agencies' processes. It is meant to serve as a guide, and not to be all encompassing, in order to allow for the unique requirements of each agency while maintaining a standard framework. OIGs should modify the document, as necessary, to fit circumstances surrounding their agency's policies, procedures, practices, and any other special situations.

B. Background

Executive orders since 1940 have directed government-wide classification standards and procedures. On December 29, 2009, President Obama signed Executive Order (E.O.) 13526, "Classified National Security Information," which establishes the current principles, policies, and procedures for classification. The E.O. prescribes a uniform system for classifying, safeguarding, and declassifying national security information. E.O. 13526 also expresses the President's belief that this nation's progress depends on the free flow of information, both with the Government, and to the American people. Accordingly, protecting information critical to national security and demonstrating a commitment to open government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

Under this order, classified information that is determined to require protection against unauthorized disclosure to prevent damage to national security must be marked appropriately to indicate its classified status. The three U.S. classification levels, and correlating-expected damage to U.S. security if the information is disclosed inappropriately, are:

- Top Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.
- Secret – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe.
- Confidential – shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information. If significant doubt exists about the appropriate level of classification, *information shall be classified at the lower level*.

Information may be classified originally or derivatively. Original classification means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Derivative classification means the incorporating, paraphrasing, restating, or generating in a 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.

Information may be originally classified only by original classification authorities (OCA): these are individuals authorized in writing, either by the President, the Vice President, or agency heads or other officials designated by the President, to initially classify information. OCAs must receive training on proper classification prior to originally classifying information and at least once per calendar year after that. To make an original classification decision, an OCA must determine if the information meets the following standards for classification:

- The information is owned, controlled, or produced by or for the U.S. Government;
- The information falls within one or more of the eight categories (reasons for classification) of information described in Section 1.4 of E.O. 13526; and
- The unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which the OCA is able to identify or describe.

If significant doubt exists about the need to classify information, it should not be classified.

At the time of original classification, the OCA must establish a specific date or event for declassification based on the duration of the information's national security sensitivity. The following information must be indicated on the document:

- The classification level (to include overall and portion markings);
- The identity of the OCA, by name and position, or by personal identifier;
- The agency of origin, if not otherwise evident;
- Declassification instructions; and
- The reason for classification.

By definition, original classification precedes all other aspects of the security classification system, including derivative classification, safeguarding, and declassification.

All personnel with an active security clearance can perform derivative classification. All personnel who apply derivative classification markings must receive training on the proper application principles of E.O. 13526 prior to derivatively classifying information and at least once every two years thereafter. Information may be derivatively classified from a source document or documents, or through the use of a classification guide. Those who perform derivative classification must:

- Be identified on the materials they derivatively classify by name and position or by personal identifier;
- Observe and respect original classification decisions; and
- Carry over to any newly-created documents, the pertinent classification markings, which include:
    - the source of the derivative classification;
    - declassification instructions;
    - overall markings; and
    - portion markings.

Authorized holders of information (including authorized holders outside the classifying organization) who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of information. In accordance with E.O. 13526 (§1.8), and its implementing directive, 32 CFR Part 2001 (§2001.14), authorized holders (including authorized holders outside the classifying agency) who want to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

Federal Government organizations that create or hold classified information are responsible for its proper management. Classification management includes developing classification guides that provide a set of instructions from an OCA to derivative classifiers that identify elements of information regarding a specific subject that must be classified and the level and duration of classification for each element. One of the most effective ways to protect classified information is by applying standard classification and control markings. Effective program management also includes comprehensive mandatory training for classifiers and a robust self-inspection program.

Federal Departments and Agencies also may have systems of control markings that identify the expansion of or limitation on the distribution of information. These markings are not classifications in and of themselves; rather, they are used to further restrict the dissemination of information to only those who have the appropriate clearance level and the need to know the information. Proposed legislation to attempt to rationalize the dissemination markings government-wide has not yet been passed into law.

The term declassified refers to the authorized change in status of information from classified information to unclassified information. Downgrading is a determination that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level. Over-classification is designated as classified information that does not meet one or more of the standards necessary for classification under E.O. 13526.

The preceding paragraphs have provided a basic introduction to the principles of classification under E.O. 13526. Individuals who conduct evaluations under P.L. 111-258 should refer to E.O. 13526 and 32 CFR, Part 2001, for a full understanding of the system to classify, safeguard, and declassify CNSI.

C. Criteria

The Reducing Over-Classification Act (Act) was intended to address issues highlighted by the 9/11 Commission about over-classification of national security information and to promote information sharing across the Federal Government and with state, local, tribal, and private-sector entities. The Act requires Inspectors General (IG) of departments and agencies within the Federal Government that have officers or employees who are authorized to make original classification decisions, in consultation with the Information Security Oversight Office (ISOO),[1] to evaluate classification management practices within those departments or agencies, to include their components.

[1] The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. ISOO is a component of the National Archives and Records Administration and receives policy and program guidance from the National Security Council.

The Act outlines the scope of the IG evaluations, establishes reporting requirements and due dates, and mandates collaboration between the IG offices performing evaluations and consultation with the ISOO on the approach that ensures that IG evaluations follow a consistent methodology, as appropriate, to allow cross-agency comparison of results.

Executive Orders and Federal Regulations:

- Public Law 111-258, "Reducing Over-Classification Act," October 7, 2010
- Executive Order 13526, "Classified National Security Information," December 29, 2009
- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
- 32 CFR Part 2001, "Classified National Security Information," June 28, 2010

[Organization] Guidance/Policy:

[Organization]

Intelligence Community Guidance/Policy:

- Intelligence Community Directive (ICD) 208, "Writing for Maximum Utility," December 17, 2008
- ICD 209, "Tearline Production and Dissemination," September 6, 2012
- ICD 710, "Classification and Control Marking System," September 11, 2009 (under revision)
- Intelligence Community Policy Guidance (ICPG) 710.1, "Application of Dissemination Controls: Originator Controls," July 25, 2012
- Intelligence Community Standard 500-21, "Tagging of Intelligence and Intelligence Related Information," January 28, 2011
- Controlled Access Program Coordination Office (CAPCO)) Intelligence Community Authorized Classification and Control Marking Register, Volume 5, Edition 1 (Version 5.1) (*Note: online version is the only authorized version*)

Other Relevant Criteria:

- ISOO Booklet, "Marking Classified National Security Information," December 2010 (Revision 1, January 2012)

D. Prior Coverage

Government Accountability Office:

- GAO Report No. LCD-80-16, "Continuing Problems in DoD's Classification of National Security Information," October 26, 1979
- GAO Report No. GAO-06-706, "DoD Can More Effectively Reduce the Risk of Classification Errors," June 30, 2006

Department of Defense

- DoD OIG Report No. 10-INTEL-09, "Assessment of Security Within the Department of Defense: Tracking and Measuring Security Costs," August 6, 2010
- DoD OIG Report No. DoDIG-2012-001, "Assessment of Security Within the Department of Defense: Training, Certification, and Professionalization," October 6, 2011

- DoD OIG Report No. DoDIG-2012-114, "Assessment of Security Within the Department of Defense: Security Policy," July 27, 2012

Environmental Protection Agency (EPA) OIG

- EPA OIG Report No. 11-P-0722, "EPA Should Prepare and Distribute Security Classification Guides," September 29, 2011
- EPA OIG Report No. 12-P-0543, "EPA's National Security Information Program Could Be Improved," June 18, 2012

E. Risks and Significance

Classification management and use of dissemination control markings are high-risk subjects which have drawn significant concern from congressional oversight committees, media, and public interest groups. Although proper classification and control of information is vital to safeguarding the nation, "over-classification," as the 9/11 Commission found, jeopardizes national security by inhibiting information sharing within the Federal Government and with state and local agencies. More recently, multiple high-profile incidents have spotlighted the release of classified government information. Such incidents have further heightened congressional, media, and public interest in classified information policy.

Classifying and controlling the dissemination of information is an inherently subjective process. Key terminology, such as "over-classification" and "damage to national security" has not been defined by E.O. 13526 or 32 CFR, Part 2001, causing those determinations to be made by personnel in the Departments and Agencies. The act of original classification requires that an OCA identify the elements of information regarding a specific subject that must be classified, describe the damage to national security that could reasonably be expected if the information is leaked, and determine how long that information needs to be protected. Derivative classifiers must interpret OCA guidance --provided in classification guides and/or derived from source documents -- to determine how to mark classified products they produce. Use of additional dissemination control marking systems are managed by agency policies. Over-classification or over-control of information is likely to increase without: strong management practices within the Departments and Agencies that have classification authority; clear implementing regulations that are consistent with the policy and procedures established by E.O. 13526; and staff that are adequately trained on the classification process.

The risk of over-classifying and over-controlling information can be mitigated by strong internal controls. The [organization] evaluation team may be able to reduce the number of documents it needs to sample if [organization] issues clear and comprehensive guidance, gives prompt updates when necessary, provides required initial and refresher training to original and derivative classifiers as required, monitors classification decisions and has a process to correct misclassification, and has an effective self-inspection program.

The risk in creating the evaluation guide is that its scope will not address some of the stakeholder concerns. Classification management is a component of information sharing which influences the number of security clearances granted, the storage and handling of classified material, the control marking systems, and declassification procedures. Therefore, it is essential to coordinate extensively with other Department and Agency OIGs that are engaged in these evaluations, and also with ISOO and relevant congressional committee staffs to ensure that the evaluation's scope and methodology are clearly defined and consistent.

II. Purpose and Objectives of Evaluation

A. Purpose

The purpose of this evaluation is to review classification management policies and practices within [organization], including [organization] components, and to assess whether existing procedures are appropriate to ensure the proper classification and marking of CNSI. This evaluation is the first of two reviews, as mandated by Congress in P.L. 111-258. The deadline for the initial evaluation is September 30, 2013, with the second evaluation due September 30, 2016.

B. Objectives

The specific objectives are to:

- Assess whether applicable classification policies, procedures, rules, regulations have been adopted, followed, and effectively administered within [organization]; and
- Identify policies, procedures, rules, regulations or management practices that may be contributing to persistent misclassification of material within [organization].

III. Scope and Methodology

A. Scope

Public Law 111-258 mandates Inspectors General of Federal departments, or agencies with an officer or employee who is authorized to make original classifications, to: (A) assess whether applicable classification policies, procedures, rules, regulations have been adopted, followed, and effectively administered within such department, agency, or component; and (B) identify policies, procedures, rules, regulations or management practices that may be contributing to persistent misclassification of material. We will include an evaluation of the policies and guidance issued by [organization] as part of the scope. The Act not only was designed to prevent over-classification of information, but the over-compartmentalization of information, while promoting sharing and declassifying information as prescribed by Federal guidelines. The evaluation will include steps, within the context of classification management, to address issues raised by the Act.

B. Methodology

This evaluation guide was prepared for all IG offices participating in this government-wide effort. It is intended to meet the requirements of P.L. 111-258 regarding the responsibilities of [organization]. As directed by the Act, we have consulted with ISOO and will coordinate throughout the evaluations with other IG offices with the intent of ensuring that our evaluations follow a consistent methodology to allow for cross-agency comparisons.

The evaluation will include reviews of relevant policies and procedures, prior OIG reports related to classification of information, and interviews with appropriate Department and Agency officials. We will obtain guidance and recommendations from the ISOO staff to help our evaluation, and coordinate with other IG offices, as appropriate. Evaluations will focus on the following eight areas (see definitions of these areas at Appendix G):

- Original classification authority;
- General program management responsibilities;
- Original classification, to include control markings;
- Derivative classification, to include control markings;
- Self-inspections;
- Reporting;
- Security education and training; and
- Intelligence Community cross-cutting issues, as applicable.

The following researchable questions for the review have been developed (when selecting the sample of documents and ultimately reporting the results, ensure that the risk-based decision(s) used is articulated – i.e., *selected X Component to review because of its high sensitivity with regard to a special national-level program*) :

1. To what extent has the [organization] adopted classification policies, procedures, rules and regulations?

a. Determine whether the [organization(s)] developed classification policies that substantially comply with E.O. 13526 and 32 CFR, Part 2001, and (if applicable) pertinent policies issued by the Office of the Director of National Intelligence (ODNI). The ISOO developed the "Agency Implementing Regulation Assessment Tool" at Appendix A to help assess compliance with E.O. 13526 and 32 CFR, Part 2001 core citations. Mapping organizational policy issuances to the checklist citations will assist in gaining a better understanding of how well the organization's policies align with E.O. 13526, 32 CFR, Part 2001, and ODNI policies.
b. Obtain, research, and document [organization] classification policies, procedures, rules and regulations relevant to E.O. 13526, 32 CFR, Part 2001, and ODNI requirements.
c. Interview [organization] officials to determine if and why classification policies, procedures, rules, and regulations needed or required have not been adopted.
d. Determine if the timing of the completion of specific organization policies and procedures is appropriate under the circumstances.
e. Determine the cause and effect of any deficiencies noted.
f. Identify recommendations for corrective actions to address deficiencies noted.

2. To what extent do the [organization] classification policies, procedures, rules and regulations comply with existing Federal classification requirements, guidelines, etc?

a. Evaluate, compare and contrast [organization] classification policies, procedures, rules, and regulations with Federal requirements, specifically E.O. 13526 and Public Law 111-258.
b. Interview appropriate officials to understand and report any discrepancies revealed.
c. Determine the cause and effect of any discrepancies noted.
d. Identify recommendations for corrective actions to address deficiencies noted.

3. **To what extent have the [organization] classification policies, procedures, rules, and regulations been effectively followed and administered?**

a. Evaluate the [organization's] compliance with training requirements.
b. Evaluate the results of the self-inspection program, and validate findings.
c. Evaluate the [organization's] compliance with classification guidance review and reporting requirements (§1.9, E.O. 13526, and §2001.16, 32 CFR Part 2001), to include a review of Fundamental Classification Guidance Review results.
d. Consult with ISOO to determine whether it conducted any prior reviews of [organization] and/or its self-assessments and reports, and any findings and recommendations that resulted.
e. Interview cognizant [organization] officials to discuss any discrepancies identified and determine the root cause of non-compliance with existing Federal classification requirements.
f. Determine the effect of any deficiencies noted.
g. Identify recommendations for corrective actions to address deficiencies noted.

4. To what extent, if any, and in what manner have information and materials been over-classified within the organization?

a. Develop a methodology to sample classified documents.
b. Obtain a sample of original and derivative classified documents to analyze.
c. Develop and use a standardized template, employing the information in the appendices to determine to what extent the classified material was appropriately classified and marked.
d. Compare the samples of original and derivative classified documents with the template to determine the extent to which information and materials may have been misclassified.
e. Interview cognizant [organization] officials to discuss any discrepancies identified and determine the root cause of any perceived misclassifications.
f. Determine the effect of any perceived deficiencies.
g. Identify recommendations for corrective actions to address perceived deficiencies.

5. To what extent, if any, and in what manner have policies, procedures, rules, regulations, or management practices contributed to any over-classifications?

a. Determine the number of items included in the sample where over-classification of original or derivative classified documents occurred.
b. Interview the [organization] officials responsible for the classification to establish a cause for the over-classification.
c. Consider what [organization] policies, procedures, rules, regulations, and management practices (i.e., training, guidance, instructions, etc.) that may have contributed to misclassification.
d. Determine the effect of any deficiencies noted.
e. Identify recommendations for corrective actions to address deficiencies noted.

IV. Appendices

Appendix A – Agency Implementing Regulation Assessment Tool

This tool is intended to help IG staffs determine if their respective organizations have adopted the essential criteria for classification management contained in the E.O. and CFR. Analysts must review agency regulations against the checklist to ensure that corresponding sections, as outlined in E.O. 13526 and 32 CFR, Part 2001, have been adequately addressed by the organization implementing regulations. A qualified response to a question, rather than a yes or no response, merits an explanation in the comments section, e.g., an agency regulation meets some requirements in a list of topics, but not all of the requirements.

Original Classification Authority

- Does the agency have Original Classification Authority [OCA]? *(Section 1.3 of E.O. 13526, § 2001.11 of 32 CFR, Part 2001)*
- Does the agency follow the standards for OCA designation? *(Section 1.3 of E.O. 13526, § 2001.11 of 32 CFR, Part 2001)*
- Does the agency report delegations of OCA authority to the Director of ISOO annually? *(Section 1.3 of E.O. 13526, § 2001.11(c) of 32 CFR, Part 2001)*

General Program Management Responsibilities

- Does the regulation cite both E.O. 13526 and 32 CFR, Part 2001, for authorizing the agency's classified national security information program?
- If the agency has special access programs, does the regulation make provisions for an annual review? (*Section 4.3 of E.O. 13526 and § 2001.60(e) of 32 CFR, Part 2001)*
- Does the Agency head or principal deputy review annually each special access program to determine whether it continues to meet the requirements of E.O. 13526? (*Section 4.3 (b) (4) of E.O. 13526)*
- If applicable, did the agency promulgate implementing regulations in the *Federal Register* to the extent that they affect the public? (*Section 5.4 (d)(2) of E.O. 13526)*
- Does the regulation require the agency to establish a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency, and to provide guidance to personnel on proper classification as needed? (*Section 5.4(d)(10) of E.O. 13526)*
- Does the regulation require the senior agency official to direct and administer the program? (*Section 5.4(d) of E.O. 13526)*
- Does the regulation require the rating of personnel on the performance of duties relating to the designation and management of classified information? (*Section 5.4(d)(7) of E.O. 13526)*
- Does the regulation provide for the suspension of OCA authority for OCAs who fail to complete OCA training annually? (*Section 1.3(d) of E.O. 13526 and § 2001.71(c)(3) of 32 CFR, Part 2001)*
- Does the regulation provide for suspending derivative classification authority for those who fail to complete training on derivative classification markings at least once every two years? (*Section 2.1(d) of E.O. 13526 and § 2001.71(d) of 32 CFR, Part 2001)*
- Does the agency ensure that the performance contract or other system used to rate civilian or military personnel performance include the designating and managing of classified information as a critical element or item to be evaluated in the rating of OCAs, security professionals, or other personnel whose duties significantly involve the handling of classified information, including derivative classifiers? (*Section 5.4 (d)(7) of E.O. 13526)*

Original Classification (Applicable only to agencies that have Original Classification Authority)

- Does the agency have a classification guide? If so, how many classification guides?
- Does the regulation cite the classification standards? (*Section 1.1 of E.O. 13526 and § 2001.10 of 32 CFR, Part 2001)*
- Is the principle regarding the presumption against classification discussed, when significant doubt exists? (*Section 1.1(b) of E.O. 13526)*
- Are the classification levels provided and only the three levels authorized for use? (*Section1.2 of E.O. 13526)*
- Is the use of classified addenda, when practicable, discussed?
- Does the agency provide procedures to safeguard, and possibly classify information, originated by non-OCAs, that is believed to be classified? (*Section 1.3 (e) of E.O. 13526)*
- Are classification categories provided and are they the only categories used? (*Section 1.4 of E.O. 13526)*
- Are duration principles provided and is emphasis placed on use of dates based on specific events? (*Section 1.5 of E.O. 13526 and § 2001.12 of 32 CFR, Part 2001)*
- Are the following items included as markings for classified documents or other media at the time of original classification, in accordance with (*Section 1.2 - 1.6 of E.O. 13526 and § 2001.12 (a-c), and § 2001.20-21 of 32 CFR, Part 2001)?*
    - Classification levels? (*Section 1.2, 1.6 (a)(1) of E.O. 13526)*
    - Identity of the OCA? (*Section 1.6 (a)(2) of E.O. 13526 and § 2001.21(a)(1) of 32 CFR, Part 2001)*
    - Agency or office of origin? (*Section 1.6 (a)(3) of E.O. 13526 and § 2001.21(a)(2) of 32 CFR, Part 2001)*
    - Declassification instructions? (*Section 1.5 (a-d), 1.6 (a)(1-4) of E.O. 13526 and § 2001.21(a)(4))*
    - Reason for classification? (*Section 1.4 and 1.6 (a)(5) of E.O. 13526 and § 2001.21(a)(3))*
    - Portion markings? (*Section 1.6 (c) of E.O. 13526 and § 2001.21 (c) of 32 CFR, Part 2001)*
    - Foreign government information markings? (*Section 1.6 (e) of E.O. 13526)*
    - Dissemination control and handling markings? (*Section 6.2 (b) of E.O. 13526 and § 2001.21(d) and § 2001.24(j) of 32 CFR, Part 2001)- <u>Note: For IC elements, dissemination markings must comply with appropriate ODNI/IC element policies and the same standards for minimum markings necessary to protect the information should be used.</u>*
    - Date of origin of the document? (*§ 2001.21(e) of 32 CFR, Part 2001)*
- Are classification markings for the electronic environment in accordance with (*Section 1.6 of E.O. 13526 and § 2001.23 of 32 CFR, Part 2001)?*
- Are classification prohibitions and limitations provided, in accordance with (*Section 1.7 of E.O. 13526 and § 2001.13 of 32 CFR, Part 2001)?*
- Has the agency established procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified? (*Section 1.8 of E.O. 13526 and § 2001.14 of 32 CFR, Part 2001)*
- Do the procedures mentioned above ensure that:
    - Individuals are not subject to retribution for such actions? (*Section 1.8 (b) of E.O. 13526, § 2001.14(b) of 32 CFR, Part 2001)*
    - An impartial official or panel is given an opportunity to review? (*Section 1.8 (b) of E.O. 13526)*

    - Individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (ISCAP)? (*Section 1.8 (b) of E.O. 13526, §2001.14(b) of 32 CFR, Part 2001)*
- Do the procedures mention timeframes? (§ *2001.14 (b) of 32 CFR, Part 2001)*
- Does the regulation contain procedures for the publication and updating of applicable security classification guides which meet the minimum standards of E.O. 13526 and Directive? (Applies only to agencies with OCA) (*Section 2.2 of E.O. 13526, § 2001.16 of 32 CFR, Part 2001)*

Derivative Classification

- Are the following topics discussed in the agency implementation regulation regarding derivative classification:
    - Assurance that the name or personal identifier of those who apply derivative classification markings is applied in a manner that is immediately apparent for each derivative classification action? (*Section 2.1 of E.O. 13526, and § 2001.22 of 32 CFR, Part 2001)*
    - Source of derivative classification to include a listing of source materials? (*Section 2.1 of E.O. 13526 and § 2001.22 (c) of 32 CFR, Part 2001)*
    - Declassification instructions? (*Section 2001.22(e) of 32 CFR, Part 2001)*
    - Marking prohibitions? (*Section 2.1 of E.O. 13526, § 2001.24 (a) of 32 CFR, Part 2001)*
    - Agency-prescribed special markings? (*§ 2001.24 (b) of 32 CFR, Part 2001 and ODNI and agency-specific criteria)*
    - Transmittal documents? (*Section 2.1 of E.O. 13526, § 2001.24 (b) of 32 CFR, Part 2001*)
    - Foreign government information? (*§ 2001.24 (c) of 32 CFR, Part 2001)*
    - Working papers? (§ *2001.24 (d) of 32 CFR, Part 2001)*

- Are the following items included as markings for classified documents or other media at the time of derivative classification, in accordance with (*Section 2.1(b)(1) E.O. 13526 and § 2001.22 of 32 CFR, Part 2001)?*
    - Identification of the derivative classifier? (*Section 2.1 of E.O. 13526 and § 2001.22(b) of 32 CFR, Part 2001)*
    - Source of derivative classification? (*Section 2.1 of E.O. 13526 and § 2001.22(c) of 32 CFR, Part 2001)*
    - Declassification instructions? (*Section 2.1 of E.O. 13526 and § 2001.22(e) of 32 CFR, Part 2001)*
    - Overall markings? (*Section 2.1 of E.O. 13526 and § 2001.22(f) of 32 CFR, Part 2001)*
    - Portion marking? (*Section 2.1 of E.O. 13526 and § 2001.22(g) of 32 CFR, Part 2001)*
    - Dissemination controls and handling markings? (*Section 2.1 of E.O. 13526 and § 2001.22(h) of 32 CFR, Part 2001)*
    - Date of origin of the documents? (*Section 2.1 of E.O. 13526 and § 2001.22 (i) of 32 CFR, Part 2001)*

Declassification.

- Does the regulation address the following topics in accordance with (*Sections 1.5, 1.6, 3.1, 3.3, 3.4, 3.5, 3.6 of E.O. 13526 and § 2001.30-34 of 32 CFR, Part 2001)?*
    - The declassification of classified information once it no longer meets the standards under E.O. 13526? (*Section 3.1 of E.O. 13526, § 2001.30 (a) of 32 CFR, Part 2001)*
    - Are procedures established to ensure the proper processing of requests to ISCAP for exemptions from automatic declassification? (*Section 3.3 and 5.3(b)(2) of E.O. 13526 and § 2001.30(m) of 32 CFR, Part 2001)*
    - For file series exemptions, does a process exist to determine that the information almost invariably falls within one of the exemption categories listed in *Section 3.3 (b) of E.O. 13526, and § 2001.30(n)(5)*? Does the process include requesting the file series exemption?
    - Development and use of declassification guides? (*Section 3.3 (j) of E.O. 13526 and § 2001.30 (k))*
    - Preparation and review of declassification guides? (*Section 3.3(j) of E.O. 13526 and § 2001.32 of 32 CFR, Part 2001)*
    - Records originated by another agency? (Referrals) (*Section 3.3 (d)(3) of E.O. 13526, § 2001.30(f) and § 2001.34 of 32 CFR, Part 2001)*
    - Restricted data and formerly restricted data (RD/FRD)? *(Section 6.2 (a) of E.O. 13526 and § 2001.30 (o) of 32 CFR, Part 2001)*
    - Does the regulation include Mandatory Declassification Review procedures and are the pertinent procedures published in the *Federal Register?* (Consult ISCAP team about its review related to all agencies' MDR programs.) (*Section 3.5 of E.O. 13526 and § 2001.33 of 32 CFR, Part 2001)*

Self-Inspections

- Does the regulation incorporate the essential elements for self-inspections in accordance with *Section 5.4 of E.O. 13526 and § 2001. 60 - 61 of 32 CFR, Part 2001?*
- Do the regulations provide for regular reviews of representative samples of original and derivative classifications and corrections of misclassifications? (*Section 5.4 of E.O. 13526 and § 2001.60(c)(2) of 32 CFR, Part 2001)*

Reporting and Definitions

- Does the agency's internal regulation incorporate the following essential elements for reporting in accordance with *§ 2001.90 and § 2001.91 of 32 CFR, Part 2001?*
    - Statistical reporting? (SF-311) (*Section 5.2 (b)(7) of E.O. 13526 and § 2001.90(b) of 32 CFR, Part 2001)*
    - Accounting for costs? (Cost Report) (*Section 5.4 (d) (8) of E.O. 13526 and § 2001.90 (c)of 32 CFR, Part 2001)*
    - Fundamental classification guidance review? (*Section 1.9 of E.O. 13526 and § 2001.91(c) of 32 CFR, Part 2001)*
    - Self-inspections? (*Section 5.5 of E.O. 13526 and § 2001.61(f) and § 2001.91(d) of 32 CFR, Part 2001)*
    - Security violations? (*Section 5.5 of E.O. 13526 and § 2001.91(d) of 32 CFR, Part 2001)*
    - Information declassified without proper authority? (*§ 2001.13(a) and § 2001.91(a) of 32 CFR, Part 2001)*
    - Do agency definitions conform with *Section 6.1 of E.O. 13526 and § 2001.92 of 32 CFR, Part 2001?*

Security Education and Training

- Does the regulation incorporate the essential elements for establishing and maintaining a formal security education and training program to include initial training, annual refresher training, specialized training, and termination briefings, in accordance with *Section 5.4 of E.O. 13526 and § 2001. 70 - 71 of 32 CFR, Part 2001?*
- Does the Agency require annual training for Original Classification Authorities? (*Section 1.3(d) of E.O. 13526, § 2001.71(c)(2) of 32 CFR, Part 2001)*
- Does the Agency require training at least every two years for individuals who apply derivative classification markings? (*Section 2.1(d) of E.O. 13526, § 2001.71(d))*
- Does the policy provide for suspending OCA and derivative classification authority for those who fail to meet the training requirements? *(Sections 1.3(d) and 2.1(d)of E.O. 13526 and § 2001.71 of 32 CFR, Part 2001)*
- Does the regulation cover the waiver process for delay in this training? *(Sections 1.3(d) and (e) of E.O. 13526 and § 2001.71(i)and (ii) of 32 CFR, Part 2001)*
- Does the training meet the requirements specified in Section 7 of P.L. 111-258?
- How does the organization track and monitor an individual's completion of required training?

Appendix B – Methodology for Determining the Appropriateness of an Original Classification Decision

This appendix is for IG staffs to review original classification decisions made by the organization to determine if the decisions were proper and follow applicable criteria.

1. Who made the decision?

a. Was the individual an original classification authority (OCA)? (§1.1 (1), E.O. Order)
b. Was the individual properly delegated the authority?
- By the President (§1.3 (a), E.O. 13526); or
- If Top Secret, by an official designated by the President (§1.3 (a) (2), E.O. 13526)
- If Secret or Confidential, by an official designated by the President pursuant to §1.3 (a) (2), E.O. 13526, or by a Top Secret OCA designated pursuant to (§1.3 (a) (3), E.O. 13526, §1.3 (c) (2), E.O. 13526)

2. Was the delegating in writing and identified the official by name or title? (§1.3 (c) (4), E.O. 13526)

3. Is the information owned by, produced by or for, or is under the control of the U.S. Government? (§1.1 (2), E.O. 13526)

4. Can the information be used in one of more of prescribed categories of § 1.4, E.O. 13526?

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 U.S., including confidential sources
e. scientific, technological, or economic matters relating to the 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 the national security
h. the development, production, or use of weapons of mass destruction

5. Can the OCA identify or describe damage to national security that could be expected in the event of unauthorized disclosure? (§1.1 (4), E.O. 13526)

a. If Top Secret, can its unauthorized disclosure be reasonably expected to cause exceptionally grave damage to the national security?
b. If Secret, can its unauthorized disclosure be reasonably expected to cause serious damage to the national security?
c. If Confidential, can its unauthorized disclosure be reasonably expected to cause damage to the national security?

6. Is the information subject to prohibitions or limitations regarding classification? (§1.7, E.O. 13526)

a. Is the information classified or otherwise marked with a distribution caveat to conceal violations of law, inefficiency or administrative error?

b. Is the information classified or otherwise marked with a distribution caveat to prevent embarrassment to a person, organization, or agency?

c. Is the information classified or otherwise marked with a distribution caveat to restrain competition?

d. Is the information classified or otherwise marked with a distribution caveat to prevent or delay the release of information that does not require protection in the interest of national security?

e. Does the information relate to basic scientific research not clearly related to national security?

f. If the information had been declassified, released to the public under proper authority, and then reclassified:

- Was the reclassification action taken under the personal authority of the agency head or deputy agency head based upon their decision that the reclassification was necessary in the interest of the national security?
- Was that official's decision in writing?
- Was the information reasonably recoverable without bringing undue attention to the information?
- Were the Assistant to the President for National Security Affairs, and Director of the Information Security Oversight Office notified of the reclassification action?
- For documents in the physical and legal custody of the U.S. National Archives and Records Administration that have been available for public use: was the Archivist of the U.S. notified of the reclassification action?

g. If the information had not previously been disclosed to the public under proper authority but was classified or reclassified after receipt of an access request:

- Does the classification meet the requirements of this order (to include the other elements of this methodology)?
- Was it accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official?

h. If the classification decision addresses items of information that are individually unclassified but have been classified by compilation or aggregation:

- Does the compilation reveal an additional association or relationship that meets the standards for classification under this order?
- Was such a determination made by an OCA in accordance with the other elements of this methodology?
- Is the additional association or relationship not otherwise revealed in the individual items of information?

7. Other ancillary issues.

a. Did the OCA establish a specific date or event for declassification? (§1.5 (a), E.O. 13526)

- If duration is greater than 10 years, was the determination made by the OCA based upon the sensitivity of the information? (§1.5 (b), E.O. 13526)

b. Were the essential markings below included? (§1.6, E.O. 13526)

- Portion marking
- Overall classification
- A "Classified by" line to include the identity, by name or personal identifier, and position of the original classifier

- A reason for classification
- A "Declassify on" line
- Appropriate use of other ODNI/agency-specific dissemination control markings

c. Did the OCA consult existing guides prior to making the original classification decision? (§2001.15 (a), 32 CFR Part 2001)

d. How was the original classification decision documented and communicated? If incorporated into a classification guide: (§2.2, E.O. 13526)

- Was the guide personally approved, in writing, by an official with program or supervisory responsibility of the information (or by the senior agency official), and who had authority to classify information originally at the highest level of classification prescribed in the guide?
- Does the guide contain the minimum prescribed information? (§2001.15 (b), 32 CFR Part 2001)
    - Identification of the subject matter of the classification guide;
    - Identification of the original classification authority by name or personal identifier, and position;
    - Identification of an agency point-of-contact or points-of-contact for questions regarding the classification guide;
    - The date of issuance or last review;
    - Precise statement of the elements of information to be protected;
    - Statement as to which classification level applies to each element of information, and, when useful, specific identification of the elements of information that are unclassified;
    - Statement, when applicable, as to special handling caveats;
    - Declassification instructions or the exemption category from automatic declassification after 25 years of existence, as approved by the ISCAP; and
    - Statement of a concise reason for classification which, at a minimum, cites the applicable classification category or categories in §1.4 of the E.O. 13526.
- Has the guide been reviewed and updated, as appropriate, at least once in the last five years? (§2001.16 (a), 32 CFR Part 2001)

e. Was the OCA appropriately trained? (§1.3 (d), E.O. 13526)

- Were essential elements covered in the training provided? (§2001.71 (c) (1), 32 CFR Part 2001)

f. Is the management of classified information included as a critical element or item in the OCA's performance evaluation? (§5.4 (d) (7) (a), E.O. 13526)

- Has the delegated OCA ever used their authority to classify? If yes, how often in the last 12 months?
- Does the OCA consider the training received, if any, satisfactory in carrying out their responsibility? If not, why not?

Appendix C – Methodology for Determining the Appropriateness of a Derivative Classification Decision

This appendix is for use by IG staff to review derivative classification decisions made by the organization to determine if the decisions were proper and follow applicable criteria. It is important to coordinate on whether a statistical or judgmental sample is appropriate for assessing derivative classification determinations.

1. Who made the decision?

a. Does the decision relate to the reproduction, extract, or summation of classified information, either from a source document or as directed by a classification guide? (§2.1 (a), E.O. 13526)

b. Are those who apply derivative classification markings identified by name and position or personal identifier? (§2.1 (b) (1), E.O. 13526)

c. Is the decision directly attributable to and does it ***precisely*** reflect an appropriate original classification decision made by an OCA, to include pertinent classification markings? (§2.1 (b) (2) (3), E.O. 13526)

2. Is the information owned by, produced by or for, or is under the control of the U.S. Government? (§1.1 (2), E.O. 13526)

3. Does the information fall within one or more of the following prescribed categories of § 1.4, E.O. 13526?

a. military plans, weapons systems, or operations

b. foreign government information

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

d. foreign relations or foreign activities of the United States, including confidential sources

e. scientific, technological, or economic matters relating to the national security

f. 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 the national security

h. the development, production, or use of weapons of mass destruction

4. Can damage to national security be expected in the event of unauthorized disclosure of information? (§1.1 (4), E.O. 13526)

a. If Top Secret, can its unauthorized disclosure be reasonably expected to cause exceptionally grave damage to the national security?

b. If Secret, can its unauthorized disclosure be reasonably expected to cause serious damage to the national security?

c. If Confidential, can its unauthorized disclosure be reasonably expected to cause damage to the national security?

5. Is the information subject to prohibitions or limitations with respect to classification? (§1.7, E.O. 13526, 32 CFR Part 2001.15 (b) (7))

a. Is the information classified or otherwise marked with a distribution caveat to conceal violations of law, inefficiency or administrative error?

b. Is the information classified or otherwise marked with a distribution caveat to prevent embarrassment to a person, organization, or agency?

c. Is the information classified or otherwise marked with a distribution caveat to restrain competition?

d. Is the information classified or otherwise marked with a distribution caveat to prevent or delay the release of information that does not require protection in the interest of national security?

e. Does the information relate to basic scientific research not clearly related to national security?

f. If the information had been declassified, released to the public under proper authority, and then reclassified:

- Was the reclassification action taken under the personal authority of the agency head or deputy agency head based upon their decision that the reclassification was necessary in the interest of the national security?
- Was that official's decision in writing?
- Was the information reasonably recoverable?
- Were the Assistant to the President for National Security Affairs, and Director of the Information Security Oversight Office notified of the reclassification action?
- Was the Archivist of the United States notified of the reclassification action for documents that have been available for public use and are in the physical and legal custody of the National Archives and Records Administration?

g. If the information had not previously been disclosed to the public under proper authority, but was classified or reclassified after receipt of an access request:

- Does the classification meet the requirements of this order (to include the other elements of this methodology)?
- Was it accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official?
- Does the classification decision address items of information that are individually unclassified but have been classified by compilation or aggregation?
- Does the compilation reveal an additional association or relationship that meets the standards for classification under the E.O. 13526?
- Was such a determination made by an OCA in accordance with the methodology for determining the appropriateness of an original classification decision?
- Is the additional association or relationship not otherwise revealed in the individual items of information?

6. Other ancillary issues not directly affecting the appropriateness of the derivative classification decision:

a. Were the essential markings below included and were they appropriately carried forward from either the source document or classification guide? (§1.6 & §2.1 (b) (3), E.O. 13526)

- Portion marking
- Overall classification
- A "Classified by" line to include the identity, by name or personal identifier, and position of the original classifier
- A "Declassify on" line
- Appropriate use of other ODNI/agency-specific dissemination control markings

b. If derivatively classified from multiple sources: (§2.1 (b) (3), E.O. 13526)

- Does the date or event for declassification correspond to the longest period of classification among the sources or markings established pursuant to §1.6 (a) (4) (D) and is it carried forward?
- Was a listing of the multiple sources provided?

c. If the classification decision was based upon a classification guide: (§2.2, E.O. 13526)

- Was the guide personally approved, in writing, by an official with program or supervisory responsibility over the information (or by the senior agency official) and who had authority to classify information originally at the highest level of classification prescribed in the guide?
- Does the guide contain the following minimum prescribed information? (§2001.15 (b), 32 CFR Part 2001)
    - Identification of the subject matter of the classification guide;
    - Identification of the original classification authority by name or personal identifier, and position;
    - Identification of an agency point-of-contact or points-of-contact for questions regarding the classification guide;
    - The date of issuance or last review;
    - Precise statement of the elements of information to be protected;
    - Statement as to which classification level applies to each element of information, and, when useful, specific identification of the elements of information that are unclassified;
    - Statement, when applicable, as to special handling caveats;
    - Declassification instructions or the exemption category from automatic declassification at 25 years, as approved by the ISCAP; and
    - Statement of a concise reason for classification which, at a minimum, cites the applicable classification category or categories in §1.4 of the E.O. 13526.
- Has the guide been reviewed and updated, as appropriate, at least once in the last five years? (§2001.16 (a), 32 CFR Part 2001)

d. Was the derivative classifier appropriately trained? (§2.1 (d), E.O. 13526)

- Were essential elements covered in the training provided? (§2001.71 (c) (1), 32 CFR Part 2001)

e. Is the management of classified information included as a critical element or item in the derivative classifier's performance evaluation if the creation or handling of classified information is a significant part of that individual's duties? (§5.4 (d) (7) (B) (C), E.O. 13526)

Appendix D – Derivative Classifier Interview Coverage

This appendix is for use by IG staff to interview [organization] personnel making derivative classification decisions to assess their knowledge of classification management procedures.

1. Introductions
2. Background (Who you represent and why you are there)
3. Questions prefaced by, "I would like to ask you some questions regarding your responsibilities as a derivative classifier and gain an understanding of your knowledge about the policies and procedures pertaining to classification management."

a. Please define a derivative classification decision that you could make and how many decisions did you make last year? (Note: If possible, obtain data from program manager about the number of derivative classification decisions recorded for personnel selected for interview.)

b. What type of training have you received regarding your derivative classification responsibilities and how often? Please provide names of courses and dates taken. Was the training adequate? If not, why not?

c. Could you explain the difference between original and derivative classification?

d. Could you explain the procedures/steps you follow in making a derivative classification decision? (Respondent should know that only OCAs can determine the level of classification and that they are to derive the level from source documents or a classification guide.)

e. Could you describe the elements that should be included in the marking of a classified document? (Response should include portion marking, overall classification markings (banner), and a classification block which includes: "Classified by", "Derived From", and "Declassify On" line entries.)

f. Does your agency have any reference material, such as a marking pamphlet, to assist in the application of classification markings?

g. Do you generally mark the documents or do you have someone else apply the appropriate markings? (If another person does this, interview that person also.)

h. In general, what is the source of the derivative classification?

- Classification Guide?
- Single source?
- Multiple sources?

i. If the source was a classification guide:

- Does your agency have one or several classification guides?
- Who approves the guide(s) and are the approvals written? (Response should be by an official with program or supervisory responsibility of the information - or by the Senior Agency Official - and who had authority to classify information originally at the highest level of classification prescribed in the guide).
- Does (do) the guide(s) contain the minimum prescribed information? (§ 2001.15(b), 32 CFR Part 2001)
    - Identification of the subject matter of the classification guide;
    - Identification of the original classifier by name or personal identifier and position;
    - Identification of an agency point of contact or points of contact for questions regarding the classification guide;
    - The date of issuance or last review;
    - Precise statement of the elements of information to be protected;
    - Statement as to which classification level applies to each element of information, and when useful, specific identification of the elements of information that are unclassified;
    - Statement, when applicable, of special handling caveats;

- Declassification instructions or the exemption category from automatic declassification at 25 years, as approved by the ISCAP;
- Statement of a concise reason for classification which, at a minimum, cites the applicable classification category or categories in §1.4 of the E.O. 13526.

j. Has the guide been reviewed and updated, as appropriate, at least once in the last five years? (§2001.16 (a), 32 CFR Part 2001)

k. If the derivatively classified document was derived from multiple sources:

- How do you determine the declassification date of the derivatively classified document?
- When creating a document or e-mail that you classify either from a document or source document, how would you establish the date and what date would you carry forward if multiple dates exist?

l. Do you attach a list of the source documents or copies of the source documents in the file with the derivatively classified document?

m. What would be your course of action if you encountered information that you believed should be classified but was not covered by a classification guide or another source document?

- Have you encountered classified information or dissemination control markings for which the reason for classification was unclear to you? If yes, what did you do? If no, what should you do in such a situation?

n. Could you describe your responsibilities related to classification challenges? (§1.8, E.O. 13526, §2001.14, 32 CFR Part 2001) Have you ever made a challenge and, if so, what was the result? Do you believe that you could make a challenge without fear of retribution?

o. Do you believe that you need additional security education training in areas that specifically relate to your duties? Do you have any suggestions for improvements?

4. Coverage Points:

a. Was the derivative classifier properly trained? (§ 2001.71(d), 32 CFR Part 2001) with regard to:

- Proper application of derivative classification markings (§2.1, E.O. 13526 and §2001.22 (a), 32 CFR Part 2001);
- Proper identification of the derivative classifier by name and position or personal identifier (§2.1, E.O. 13526 and §2001.22 (b), 32 CFR Part 2001);
- Proper identification of source information of the "Derived From Line," including the use of multiple sources (§2.1, E.O. 13526 and §2001.22 (c), 32 CFR Part 2001);
- Proper declassification markings (§2.1, E.O. 13526 and §2001.22(e), 32 CFR Part 2001);
- Proper use of the compilation or aggregation of information (§ 1.7(e), E.O. 13526);
- Reclassification of information (§ 1.7, E.O. 13526 and § 2001.13, 32 CFR Part 2001);
- Challenge provision of the E.O. 13526 (§ 1.8, E.O. 13526 and § 2001.14, 32 CFR Part 2001).

b. Is the management of classified information included as a critical element or item in the derivative classifier's performance evaluation? (§ 5.4 (d) (7) (B) (C), E.O. 13526)

c. Does the individual you interviewed seem to have enough knowledge about classification management to be reasonably expected to make appropriate derivative classification decisions?

d. Does the individual you interviewed appear to understand the overall direction of the order that protecting classified information and sharing information, as appropriate, are equally important objectives?

e. Does the individual you interviewed believe that the organizational leadership offers a culture and tone that emphasizes proper classification and is open to challenges, if needed, to correct its system of classification?

5. Do derivative classifiers have any elements in their performance report related to classification management?

Appendix E – Original Classification Authority (OCA) Interview Coverage

This appendix is for use by IG staff to interview [organization] personnel making original classification decisions to determine their knowledge of classification management procedures. It is intended to help gauge whether the OCA should have this authority and if that individual has expert knowledge of the information to ensure that information is not over-classified.

1. How would you estimate how many classification decisions you made in the last year?
2. What is your familiarity with OCA responsibilities to include training you have received in original classification?
3. Are you required to receive and have you received annual training on classification management? What is your opinion of the quality of the training and does it address proper application of classified markings?
4. What is the result if you do not receive annual training (e.g., an unauthorized release of classified information and/or an adverse personnel action against the OCA)?
5. Does your agency have a classification guide which covers the classified information that you usually work with? What was your role in supporting the classification guide and what were your thoughts on its completeness?
6. Do you and your organization adequately balance the need to classify information with the need to share it with those who need it and encourage challenges, and possibly a correction, to a classification decision? (If yes, please state how. If no, please state why not.)
7. Is damage to national security described in a manner that enables derivative classifiers to consistently apply the definition throughout your organization?
8. Have you encountered classified information which you believe to be over-classified or over-controlled? If yes, what did you do? If no, what should you do in such a situation?
9. What are your responsibilities if your classification decision is met by an access demand or challenge?
10. Have you ever challenged the classification level or control markings of a particular document?
11. What is your understanding of the E.O. 13526's classification prohibitions and limitations?
12. Is the OCA aware of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure?
13. What are your ideas on providing incentives to challenges to misclassification?
14. Does the OCA believe that pervasive over-classification exists in the organization? Do problems exist with the system of dissemination controls? If so, why?
15. Discuss any challenges that the OCA sees in classification management and how would this individual address them?

Appendix F – Additional Criteria and Questions for Intelligence Community Components

This appendix is for use by IG staffs that are part of an IC component or that cover an IC element within their respective organization. It is intended to help determine if your respective IC element has adequately implemented appropriate ODNI-issued IC guidance related to classification management and classification and control markings. It will also help determine if your work indicates the existence of ODNI-issued IC policies, procedures, rules, regulations, or management practices that may have or are contributing to persistent misclassification within your organization or that have resulted in the lack of access to ODNI-produced classified documents or information. The Appendix is also intended to gain an understanding about whether – and the extent to which – national intelligence information is being provided to appropriate parties without delay or unnecessary restrictions.

1. Among other items, IG elements should ensure that classification management within their respective organizations is consistent with any IC-wide guidance pertaining to:
   - P.L. 111-258, Section 5
   - E.O. 13526, Sections 3.1(c), 3.5(f), 4.1(f-g), 4.3, 5.1(c), and 6.2(b)
   - 32 CFR, Part 2001
   - Intelligence Community Guidance identified in Section C of this guide and updated by IC IG audit team (*Note: Several new ODNI publications are in draft*)
2. Identify all ODNI-issued IC criteria (i.e. Intelligence Community Directives (ICD), Intelligence Community Policy Guidance (ICPG), Controlled Access Program Coordination Office (CAPCO) Register and Manual, etc) cited by your organization policy and provide to DoD and IC IG teams. Determine if the ODNI has provided your respective organization with any other instructions pertaining to classification management or classification and control markings.
   - Does your organization have access to electronic versions of updated policies and manuals? For example, CAPCO states that the only official Register and Manual is the electronic version, yet not all elements have ready access to CWE or Joint Worldwide Intelligence Communication System. Are all elements able to access CAPCO's unclassified sharepoint site?
   - Do any other IC criteria exist that you have trouble accessing or for which your organization does not receive updates?
3. Interview organization personnel to determine if any delays in the issuance of relevant ODNI-issued IC policies or guidance has delayed implementing policies and procedures at the IC components. (*Note: Several new ODNI IC publications are in draft and we would like to determine if any publications require significant change in your classification management programs*).
4. Interview organization classification management officials to determine what role, if any, they believe ODNI has over their organization regarding classification management of intelligence information, to include standard formats and portion markings to enhance information sharing, training, performance standards, and dissemination and control markings.
5. Has your work identified any issues related to ODNI SCI-controlled access information? If so, what are they?
6. Do any issues or concerns exist regarding the CAPCO Register and Manual? Does your organization use any markings outside the register? If so, when and why and is such use compliant with ODNI policies?

7. Has your work identified any issues pertaining to performance elements or training that you have attributed to inadequate or lack of policy by the ODNI?
8. Does your organization participate in any IC working groups pertaining to classification management and dissemination control markings? Do any issues or concerns exist with this participation? Do your representatives feel empowered to speak for their organizations? If not, why not?
9. Compare ODNI-issued IC requirements to organization policies and determine if ODNI policies, procedures, rules, and regulations were adopted. Assess potential impact of adopting recently issued or draft guidance.
10. As part of testing of OCA and derivative classification decisions, determine if the relevant ODNI-issued IC policies, procedures, rules, and regulations were followed. If not, why not? Please provide specific details.
11. Has your work identified any problems/concerns with ODNI responding timely to classification markings or dissemination control marking challenges? If so, please provide details.
12. Has your work identified any issues or concerns related to any over-classified, misclassified or over-controlled ODNI document? If so, did your organization challenge the classification level or dissemination control marking and what was the response?
13. Does your field work show that any ODNI policies, procedures, rules, regulations, or management practices contributed to persistent misclassification of documents within your organization? For purposes of this question, consider both the classification level and the control markings.
14. A report issued by the ODNI, "Intelligence Community Classification Guidance Findings and Recommendations Report," January 2008, provided recommendations intended to move the IC towards common IC guidelines that would transcend organizational culture. Based on your assessment of relevant classification guides in your organization compared to guides issued by other IC elements, are any significant benefit/efficiencies gained (pros and cons) by ODNI leading an effort to further standardize classification guides in the IC? The intent is three-fold to move to (or as close as possible) a single capstone classification guide that would standardize the framework (organization, style, definitions, etc.) of all guides, provide standard definitions for the concepts behind the information that needs to be protected, and to help describe "damage" to national security.

Appendix G - Definitions

Original Classification Authority means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to initially classify information.

General program management responsibilities refer to the responsibilities of Departments and Agencies implementing the program under E.O. 13526. These include the responsibilities of the agency head to support the program and the responsibilities of the senior agency official (SAO), whom the agency head has designated to direct and administer the program. Among the SAO's responsibilities are:

- Overseeing the program established under E.O. 13526;
- Issuing implementing regulations;
- Establishing and maintaining security education and training programs;
- Establishing and maintaining an on-going self-inspection program;
- Ensuring that the designation and management of classified information is included as a critical rating element in the systems used to rate OCAs, security managers or security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information, including those who apply derivative classification markings; and
- Establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification, as needed.

Original classification means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Derivative classification means the 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.

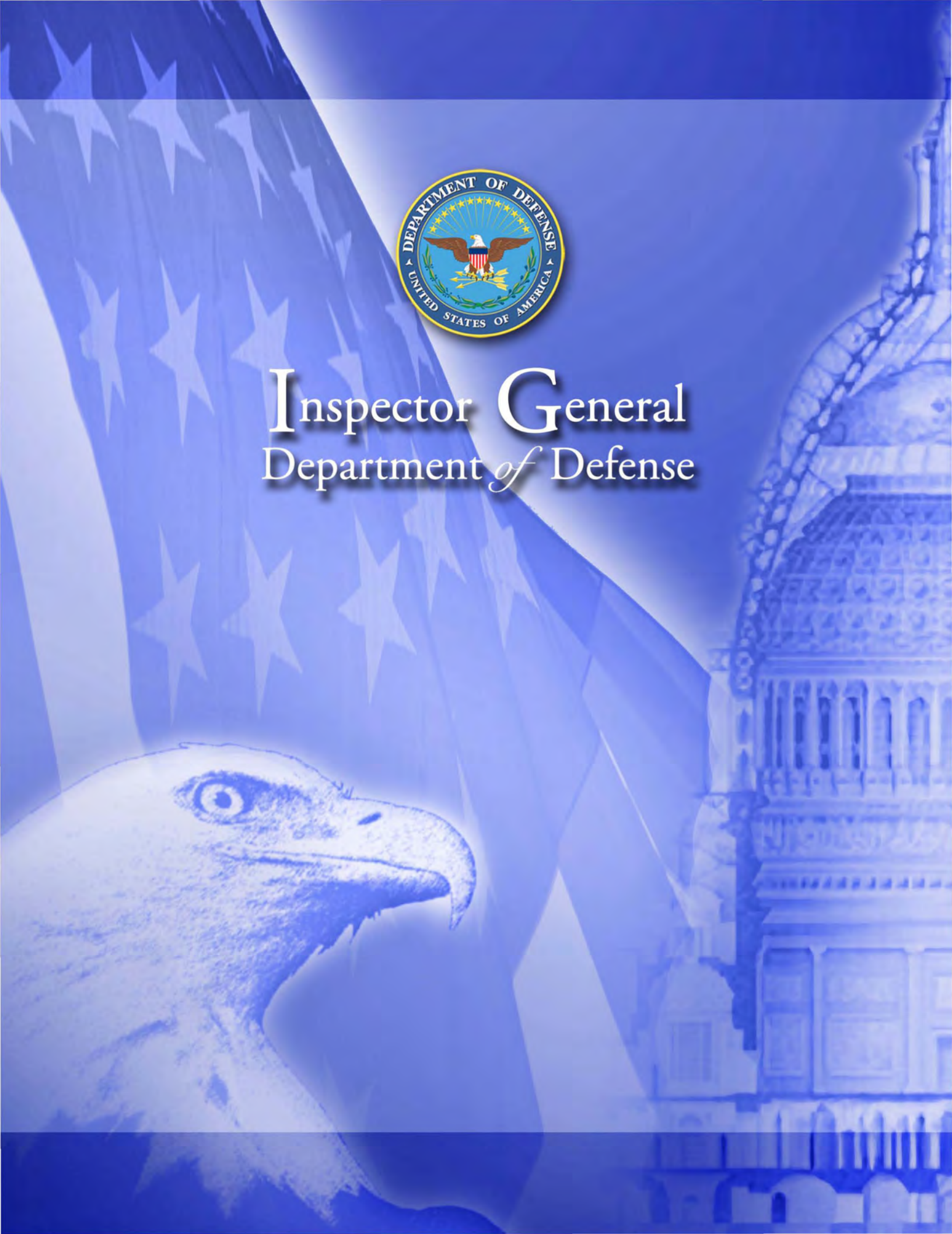
Declassification means the authorized change in the status of information from classified information to unclassified information.

Self-inspections means the internal review and evaluation of individual agency activities and the agency as a whole with respect to carrying out of the program established under E.O. 13526 and its implementing directives.

Reporting and definitions. Reporting refers to information that Departments and Agencies are required to report to ISOO on an annual basis, or as circumstances require. Among these requirements are statistical reporting of classification activity, accounting for costs, fundamental classification guidance review, self-inspections, and security violations. A complete list can be found in 32 CFR Part 2001.90. Definitions are outlined in E.O. 13526, Section 6.1, and 32 CFR, Part 2001.92.

Security education and training is an educational program that encompasses initial training, annual refresher training, and specialized training. It includes training for OCAs and those who apply derivative classification markings and termination briefings that are designed to:

- Ensure that all executive branch employees who create, process, or handle classified information have a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies and procedures;
- Increase uniformity in the conduct of agency security education and training programs; and
- Reduce instances of over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices.



Inspector General
Department of Defense