Office of the Director of National Intelligence

Principles of Classification Management for the Intelligence Community

Leading Intelligence Integration

PRINCIPLES OF CLASSIFICATION MANAGEMENT FOR THE INTELLIGENCE COMMUNITY

1) Risk Management:

Classification decisions should reflect a risk management strategy; classification policy should address how the strategy is applied in defining and differentiating classification levels. Fundamental principle – Passage of time diminishes sensitivity of some classified information.

2) Classification Levels:

E.O. 13526 cites three classification levels – Top Secret, Secret, and Confidential – characterized by the extent of damage reasonably expected to occur as a result of the unauthorized release of information.

3) Unclassified Information:

Classification policies should elucidate the reasoning agencies employ in determining whether information over which they have Original Classification Authority is Unclassified, Controlled Unclassified, or Classified.

4) Classification Categories and Marking Guidance:

Classification policies should convey how classification levels and markings are used to manage information, facilitate information sharing, and achieve mission objectives while appropriately protecting CNSI.

5) Declassifying and Downgrading Classified Information:

These are integral components of classification management and should be reflected in classification policies.

6) Information Sharing with Foreign Governments:

Classification policies should abet greater integration of information sharing and safeguarding with foreign partners, consistent with U.S. law and protection of sensitive information, sources, and methods.

7) Implementation:

All IC roles, resources, processes, and policies should be aligned to support robust implementation of these principles, consistent with applicable laws, Executive Orders, and directives.

PURPOSE

The *Principles of Classification Management for the Intelligence Community (IC)* are intended to facilitate and align IC decisions on classifying and marking Classified National Security Information (CNSI), particularly categories of CNSI common to multiple agencies. They articulate general norms that IC elements will follow in implementing their authorities when classifying and marking intelligence information, products, and reports.[1] Classifying and marking CNSI accurately and consistently are critical to ensuring accountability and transparency throughout the Community. The requirement to do so will grow in importance as the IC moves increasingly into an era of shared data and must respond to new technology that is enabling and changing ways information is communicated.[2] These *Principles* apply to the entire IC and should be incorporated by agencies in their classification guides. They also can be used by other agencies as a benchmark in establishing their classification programs.

The *Principles of Classification Management* do not establish new classification standards or requirements; modify or supersede applicable laws or executive orders and directives, including Executive Order (E.O.) 13526, *Classified National Security Information*, or information classified under the Atomic Energy Act;[3] nor do they abrogate or alter the exercise of Original Classification Authority (OCA) by officials identified in Section 1.3 (a) of the Order.[4]

[1] Authorities are derived from the National Security Act of 1947, as amended; Executive Order (E.O.) 12333, as amended; E.O. 13526; 32 CFR Part 2001; and other applicable provisions of law. The principle of, "accurate and accountable application of classification standards and routine" is mandated in E.O. 13526.

[2] Intelligence Community Directive (ICD) 710, *Classification Management and Control Markings System*, governs the implementation and oversight of the IC classification management and control markings system.

[3] The classification principles and requirements for information classified under the Atomic Energy Act (Restricted Data [RD], Formerly Restricted Data [FRD], and Transclassified Foreign Nuclear Information [TFNI]) are contained in 10 CFR Part 1045, Nuclear Classification and Declassification. These include unique authority for the initial classification and declassification of RD; classification, marking, and declassification of matter containing RD, FRD, and TFNI; and limits on the transmission of RD and FRD to foreign governments.

[4] In 2016, the DNI asked IC elements to evaluate the number of officials they have possessing OCA to ensure it is the minimum needed to meet mission requirements.

RISK MANAGEMENT

All agencies should reflect in their classification decisions a Risk Management strategy—mitigating the likelihood and severity of risk—in protecting classified information over which they have OCA, including clear descriptions in their classification policies of how the strategy is used when making classification determinations.[5] The strategy is based in part on the principle that all information should be marked at the lowest level of classification consistent with its appropriate protection and handling. A Risk Avoidance strategy—eliminating risk entirely—is not an acceptable basis for agency guides because it encourages over-classification, restricts information sharing, hinders the optimal use of intelligence information in support of national security and foreign policy goals, and is contrary to E.O. 13526 and the *Principles of Intelligence Transparency for the Intelligence Community*.

A Risk Management strategy in classifying and marking CNSI should incorporate three key determinations: ***Threat***—the degree of danger of information compromise; ***Value***—the significance of the information to national security and foreign policy goals; and ***Vulnerability***—the degree of difficulty in acquiring the information; the availability of alternative, comparable sources for the information; and the damage caused if the information enters the public domain or is covertly obtained by adversaries.

[5] IC policy for the protection of classified national intelligence, including sensitive compartmented information, is contained in ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information.*

CLASSIFICATION LEVELS

The three classification levels approved for use in Section 1.2 of E.O. 13526 are Top Secret, Secret, and Confidential.[6] They are differentiated in the Order by the extent of damage reasonably expected to occur as a result of the unauthorized release of information at each level, respectively:

- Top Secret: Exceptionally grave damage to the national security
- Secret: Serious damage to the national security
- Confidential: Damage to the national security

Based on this taxonomy, agencies' classification policies—as represented in their classification guides—should interpret and illustrate the varying amount of damage caused by the unauthorized release of information at each of the levels to enable derivative classifiers to understand and distinguish between them in rendering accurate and consistent classification decisions.

Enhancing specificity should facilitate more consistency across the Community in defining and applying classification levels, thereby providing greater fidelity for the reasoning that agencies employ to determine the appropriate marking for CNSI over which they have OCA.

[6] The IC is currently studying the feasibility of eliminating the CONFIDENTIAL classification level to determine if it can be done without negatively impacting operational effectiveness.

UNCLASSIFIED INFORMATION

Agencies' classification policies should identify the categories of information over which they have OCA that are Unclassified. This is not intended to duplicate the purpose of a declassification guide, which promulgates standards for evaluating whether previously classified information can be declassified. Instead, it elucidates how agencies determine which information they control is originally Unclassified, highlighting clearly what distinguishes it from information that requires classification.

E.O. 13556, *Controlled Unclassified Information* (CUI), established an open and uniform program for managing unclassified information that requires safeguarding or dissemination controls. Agencies' guidance for CUI must be consonant with ISOO's rule, published in the Federal Register (32 CFR Part 2002, 14 September 2016), establishing policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI; self-inspection and oversight requirements; and other facets of the CUI program.

CLASSIFICATION CATEGORIES AND MARKING GUIDANCE

Agencies' classification policies should encompass all categories of classified information over which they have OCA. Guidance derived from the policy should make clear the criteria used to assess—individually and comparatively—levels of sensitivity and how variations in sensitivity are reflected in classification controls for safeguarding and disseminating agencies' OCA-originated information. The criteria should make readily discernible why, for example, certain categories of information must be protected at Top Secret, while others warrant a different marking. Such clarity enhances understanding of how the IC uses classification levels and markings to safeguard information, facilitate information sharing, and achieve mission objectives while adhering to the provisions of the E.O. 13526 and ODNI policies on the management and protection of CNSI.

Classification guides should adopt a uniform framework in organizing and presenting instructions on classifying categories of intelligence information, thereby providing consistency in how the guidance is written, structured, and understood across the IC. This is especially important for common categories of CNSI over which multiple agencies have OCA. Guides should include for each category of classified information: a list of the different elements/items of classified information within the category, a classification level and reasons for the level, and any remarks that furnish additional clarity to users in classifying CNSI.[7] With adoption of a common version of the Classification Management Tool throughout the Community as part of the IC Information Technology Enterprise (IC ITE), standardizing the categories, levels and rationales for classifying intelligence will become increasingly important in ensuring proper information sharing and protection.

[7] The table in the Appendix identifies the essential elements of information guides should contain in classifying categories of CNSI. Agencies determine the format used in organizing and arraying such information in their guides and are not required to use a table.

DECLASSIFYING AND DOWNGRADING CLASSIFIED INFORMATION

Declassifying and downgrading CNSI are integral components of classification management, as mandated in E.O. 13526.[8] All agencies should have policies governing these activities as part of their classification management processes. That the passage of time diminishes the sensitivity of some classified information is a fundamental principle of a Risk Management strategy; agencies should use this consideration in evaluating the duration of the requirement to protect information, as acknowledged in Section 1.5 of E.O. 13526. In addition to affirming the importance of declassification and downgrading as primary elements of classification management, agencies should be proactive and clear in identifying the oversight and compliance mechanisms they use to ensure declassify/downgrade decisions over which they have OCA are made correctly and in a timely fashion. Factors that could affect the continuing need to protect information—such as revisions to U.S. foreign policy goals, changes in threats to U.S. national security, and the extent to which information is already in the public domain—should be considered when assessing changes to classification guidelines. Updates to classification guides based on these and other factors should be consistent with a risk management strategy in classifying and marking CNSI.

Incorporating declassification guidance in a classification guide is not intended to supplant the role and function of a declassification guide. Its purpose is to add further clarity and consistency to the processes and standards by which agencies make publicly available information that no longer requires protection, and balancing that objective with the simultaneous need to safeguard information that must remain withheld from public release.

[8] The Order defines three declassification programs – systematic, automatic, and mandatory. While acknowledging the constraining effect resource limitations can have on declassification efforts, the DNI has expressed his support for IC elements establishing or expanding existing proactive, discretionary declassification programs to increase the amount of material made available to the public.

INFORMATION SHARING WITH FOREIGN GOVERNMENTS

Foreign disclosure and release actions can provide critical support to national security and foreign policy objectives. Capabilities to share information with foreign partners, particularly FVEY countries, will expand by means of IC ITE and the IC Desktop Environment. Classification policies should be written to abet greater integration of intelligence information sharing and safeguarding with foreign partners, while remaining consistent with U.S. legal and policy requirements and the protection of sensitive information, sources, and methods.

To maximize appropriate information sharing with foreign partners, agencies' policies on foreign disclosure and release control markings must be consistent with ICD 403, *Foreign Disclosure and Release of Classified National Intelligence*, and IC Policy Guidance (ICPG) 710.2, *Application of Dissemination Controls: Foreign Disclosure and Release Markings*. Agencies should have oversight and compliance mechanisms to ensure use of the NOFORN dissemination control marking is limited to the minimum necessary. Classification guides should incorporate the principle that use of NOFORN as a dissemination control marking must be evaluated case-by-case (e.g., disseminated analytic products, memoranda, and e-mails). Guidance should include explicit criteria that explain and limit when the NOFORN marking is appropriate to prevent the release of CNSI to foreign governments. Agencies' foreign disclosure and release policies should balance the importance of seeking to share classified information with foreign partners with the requirement to adhere to the provisions of ICPG 403.1, *Criteria for Foreign Disclosure and Release of Classified National Intelligence*.

IMPLEMENTATION

All IC roles, resources, processes, and policies should be aligned to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives.

APPENDIX

Table: Illustrative Framework for Organizing, Presenting, and Classifying Categories of Intelligence and Intelligence-Related Information in Classification Guides

Category	Element/ Item	Classification Level/ Dissemination Control(s)	Rationale	Remarks
Associations/ Relationships				
Sources/ Methods/ Capabilities				
Resources				
Access				
Safeguards				

171616 ID 02-17