The Office of the Director of National Intelligence
Associate Director of National Intelligence
and Chief Information Officer

INTELLIGENCE COMMUNITY CLASSIFICATION GUIDANCE FINDINGS AND RECOMMENDATIONS REPORT

January 2008

Prepared by

The Director of National Intelligence and Chief Information Officer,
Intelligence Community Technology Governance

Table of Contents

FOREWORD

The Director of National Intelligence (DNI) directs an aggressive schedule of initiatives to enhance the effectiveness of the Intelligence Community and better serve the nation. He believes that the Intelligence Community must become more agile and effective by enhancing community integration and collaboration. To this end, he targeted accelerated information sharing as a primary transformational goal for the Intelligence Community.

A critical component of effective intelligence collaboration and information sharing is a common understanding of information classification standards and policies. Inconsistent interpretation and application of the classification levels defined by Executive Order 12958, as amended, often results in uneven guidance, misunderstanding, and a lack of trust between Intelligence Community agencies and mission partners concerning the proper handling and protection of information. Agency-unique or contradictory classification guidance can slow or prevent information sharing across agency, government, and partner lines. Therefore, we must create classification guidelines that transcend organizational cultures. True information sharing and intelligence collaboration cannot occur until all participants trust that when they provide information it will be appropriately protected. A capstone Intelligence Community classification guide governing intelligence information is necessary to enable that trust.

Sherrill L. Nicely 25 January 2008

Sherrill L. Nicely
Deputy Associate Director of National Intelligence
for Intelligence Community Information Technology Governance

EXECUTIVE SUMMARY

In 2006, the Associate Director of National Intelligence and Chief Information Officer (ADNI&CIO) initiated an effort to develop a classification guide that could be used by the entire Intelligence Community. He established a team to review and analyze classification guides provided by Intelligence Community agencies, solicit input from the Community at large, and provide findings and recommendations for developing one common Intelligence Community Classification Guide.

The team found that the reviewed classification guides often provided little insight into the reasons for setting classification and limited guidance for discriminating between classification levels. Most of the guides were agency- or program-specific. In situations where users perceived conflicting guidance, they found it difficult to discern which classification guide or level should take precedence, leading to over-classification in many cases.

Investigation into the meaning of classification, as well as the history of security and classification reform efforts, yielded interesting points to consider when designing the Intelligence Community Classification Guide. The team also considered additional factors, such as future requirements from the Program Manager, Information Sharing Environment (PM-ISE).

This report presents a short background of the Intelligence Community Classification Guide effort, the methodology used to compile and analyze the agency classification guides information, and the program team's findings and recommendations. The discussion herein naturally extends beyond the content of classification guides to the basis upon which Federal Government employees make classification determinations and the manner in which such guidance should be maintained to enable timely, authoritative guidance across the community of intelligence users and producers. This analysis provides the baseline for the next phase of this effort—development of a capstone Intelligence Community Classification Guide.

PURPOSE

This *Intelligence Community Classification Guidance Findings and Recommendations Report* presents the findings and recommendations that resulted from assessing the similarities and differences among Intelligence Community and related classification guides in order to create one common Intelligence Community Classification Guide.

BACKGROUND

A critical component of Intelligence Community collaboration and information sharing is a common understanding of information classification standards and policies. Classification guides describe the level of classification, the legal justification for the classification, and the instructions regarding declassification of the information in the future. Federal Government agencies base their classification guides on language from a few key documents, which contain necessarily broad language. Many interpretations exist concerning what constitutes harm or the degree of harm that might result from improper disclosure of the information, often leading to inconsistent or contradictory guidelines from different agencies.

Basis for Classifying Information

Throughout the history of the United States, certain information has been held "in confidence" to protect national security. Executive Order (E.O.) 12958, as amended, specifies conditions under which information may be classified for reasons of national security. Information is eligible for classification only if it meets all of the following conditions:

(1) *an original classification authority is classifying the information;*

(2) *the information is owned by, produced by or for, or is under the control of the United States Government;*

(3) *the information falls within one or more of the categories of information listed in section 1.4 of this order; and*

(4) *the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.*[1]

Furthermore, Section 1.4 of E.O. 12958, as amended, states that *information shall not be considered for classification unless it concerns:*

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

[1] Part 1, Section 1.1(a) of E.O. 13292, "Further Amendment to Executive Order 12958, as amended, Classified National Security Information," March 25, 2003. Cited in Federal Register, Vol. 68, No. 60, March 28, 2003.

(b) foreign government information;

(c) intelligence activities (including special activities), 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, which includes defense against transnational terrorism;

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

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(h) weapons of mass destruction.[2]

Thus, according to the President of the United States, only information owned by, produced for, or under the control of the U.S. Government that could cause harm *if disclosed in an unauthorized manner* and contained in one of the eight categories listed above (Section 1.4 a through h) *may* be classified.

Levels of Classification

E.O. 12958,[3] as amended, delineates three classification levels that describe the degree of potential harm to U.S. national security that could result if the information were to be disclosed in an unauthorized manner:

- **Confidential –** Unauthorized disclosure of this information could be expected to cause "damage" to the national security.
- **Secret –** Unauthorized disclosure of this information could be expected to cause "serious damage" to the national security.
- **Top Secret –** Unauthorized disclosure of this information could be expected to cause "exceptionally grave damage" to the national security.

E.O. 12958, as amended, requires that the original classifying authority (OCA) be able to "identify or describe the damage to the national security" that resulted in a classification decision. However, neither E.O. 12958, as amended, nor the implementing regulation promulgated by the Information Security Oversight Office (ISOO) of the National Archives and

[2] Section 1.4 of E.O. 12958, As Amended, March 25, 2003.

[3] Section 1.2 of E.O. 12958, As Amended, March 25, 2003.

Records Administration (NARA)[4] provide further definition as to what constitutes "damage" or "national security."

Relationship of Information Classification to Information Sharing

Following the terrorist attacks of September 2001, the President of the United States directed the Intelligence Community to transition from a *"need-to-know"* to a *"need-to-share"* philosophy.[5] In March 2007, the Director of National Intelligence (DNI) announced the creation of an Information Sharing Steering Committee (ISSC) to move the Intelligence Community beyond the *"need to share"* to a *"responsibility to provide"* philosophy.[6] Requirements to streamline and standardize information sharing guidelines to increase efficiency and authorized access to information accompanied this announcement. However, the DNI is responsible for protecting intelligence sources and methods, and protection of intelligence sources and methods is the issue most often cited as a barrier to information sharing.

More opportunities exist than ever before to provide meaningful intelligence products that are protective of the sources and methods used to acquire the information. In the current Intelligence Community Information Sharing Environment (ISE), analysts and "watch" personnel rapidly share these products across multiple classification domains and operating systems with a variety of partners, ranging from foreign intelligence services and formal treaty members to federal, state, or local government task forces to law enforcement officials and emergency response personnel. The constant shift of personnel and the ad hoc nature of these intelligence partnerships demand increased nimbleness and flexibility in communications than in the past. Information must flow between domains in a manner that is unconstrained and protects that which should properly remain controlled.

The information-sharing needs (i.e., to rapidly receive and transmit meaningful intelligence products) of the "customers" call into question the current methods of classifying and sharing intelligence information. As the primary collector and analyzer of national security and counterterrorism information, the Intelligence Community plays a major role in transforming the ISE.

A common understanding of classification standards and policies is critical to information sharing and collaboration. Inconsistent or contradictory classification rules that confuse users may slow or prevent information sharing. A set of classification standards common to all members of the Intelligence Community should minimize such problems in the future.

---

[4] National Archives and Records Administration Information Security Oversight Office, "Classified National Security Information Directive No. 1: Final Rule," 32 Code of Federal Regulations (CFR), Parts 2001 and 2004, September 23, 2003.

[5] The White House. "Message to the Congress of the United States on Information Sharing," December 16, 2005.

[6] DNI. "Creation of New Information Sharing Steering Committee for the Intelligence Community," ODNI News Release No. 06-07, March 6, 2007.

Déjà Vu: Call for Change in Classification Practices

The 1994 Joint Security Commission's (JSC) report, "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence," called for "consistent and coherent" security policies and practices "across the Defense and Intelligence Communities."[7] The JSC also described the classification system as "cumbersome and confusing," "inherently subjective," and "more complex than necessary."[8] Furthermore, the JSC suggested that simplifying the information classification system would simplify the entire security system.[9] Also within this report, the JSC stressed the need for a risk-management approach to providing "security system" standards, as well as the need to balance security with cost considerations. The JSC's subsequent report, "Report by the Joint Security Commission II," focused on the cost issues associated with security enforcement and information protection.[10] The Intelligence Community initiated changes in response to the Commission's recommendations; however, it did not adopt a more simplified security structure. Not surprisingly, classification/dissemination/ disclosure problems continue.

Enhanced collaboration and integration are the Intelligence Community's current maxims. The Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA), the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction final report, the "National Intelligence Strategy of the United States," and reports by the Markle Foundation identify collaboration and integration as critical goals. These reports frequently prescribe technological solutions, as well as "sustained leadership and strong oversight."[11]

Several of these documents call for development of policies and clarification of authorities to facilitate information sharing. One study stated: "[the] government must rethink its approach to calculating and managing the risks involved with sharing sensitive security information."[12] The primary difficulty in defining policies to facilitate information sharing has been in determining who holds the authority to force sharing of sensitive classified information in an environment of distributed classification authorities. No consensus has been achieved nor has such an authority been established to enforce guidelines across agency and intelligence discipline lines.

All recent studies acknowledge the need for change in the information-sharing system. They tacitly, if not explicitly, accept the need for classified information; they do not question the role of classification in the protection of national security nor the process by which information is determined to be "classified." There has been no demand to review the elements involved in

---

[7] Joint Security Commission (JSC). "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence," February 28, 1994. (Cited hereafter as "JSC, 'Redefining Security'.")

[8] JSC, "Redefining Security," 7-9.

[9] JSC, "Redefining Security," 11.

[10] JSC, "Report by the Joint Security Commission II," August 24, 1999.

[11] Markle Foundation Task Force, "Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment," July 2006. (Cited hereafter as "Markle.")

[12] Markle, 20.

identification, justification, labeling, and management (protection from unauthorized disclosure) of classified information throughout its life-cycle.

METHODOLOGY

The Intelligence Community Classification Guide team requested capstone classification guides from the primary Intelligence Community agencies: Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA). The team also requested classification guides from the Department of State (DOS) and the Federal Bureau of Investigation (FBI) because these agencies have unique needs and perspectives. In addition, the team reviewed policies and guidance from the Department of Homeland Security (DHS), a Continuity of Operations exercise classification guide, and Intelligence Community directives.

The team reviewed the contents and organization of these classification guides. Since no two guides were alike in organization, format, or writing style, the team produced a framework into which the team compiled each guide's entries. The team then used five broad categories to organize the entries:

- Mission Enabling Functions (i.e., organization management and support functions).
- Emergency Planning.
- Relationships (i.e., those among agencies and organizations).
- Operations and Intelligence Activities (i.e., the "acquisition" of information).
- Information and Data (i.e., the "content" of analysis).

The team compiled, reformatted, and placed all entries from the parent classification guides into the new framework to facilitate content analysis. The team also included in the framework all of the originating organizations' caveats, descriptions, releasability information, and declassification instructions.

FINDINGS AND RECOMMENDATIONS

Analysis of the Community's classification guides revealed both strengths and weaknesses in presentation as well as underlying issues contained in the guidance for classification decisions. The following sections highlight the main areas of concern and provide the team's findings and recommendations, based upon its detailed analysis of the Intelligence Community's classification guides.

Classification and "Damage" Levels

Findings

- There appears to be no common understanding of classification levels among the classification guides reviewed by the team, nor any consistent guidance as to what constitutes "damage," "serious damage," or "exceptionally grave damage" to national security—nor is it clear what simply needs to be protected from broad public dissemination (unclassified but for official use only). There is wide variance in application of classification levels.
- The definitions of "national security" and what constitutes "intelligence" — and thus what must be classified — are unclear. Boundaries between foreign and domestic information, as well as intelligence and law enforcement, are blurred.

Recommendations

- Provide meaningful definitions of classification levels, including identifiable reasons or rationales for classifying or not classifying information.
- Provide meaningful definitions of "damage levels" and correlations to classification levels to allow original classification authorities (OCAs) to more readily determine the risk of damage associated with unauthorized disclosure of information. Use security categories in a manner similar to that of Federal Information Processing Standard (FIPS) Publication (PUB) 199 by describing damage levels correlated to potential impacts on an organization's capability to accomplish its assigned mission, protect assets, maintain day-to-day functions, and protect both individuals and the nation's classified information and data.
- Define the damage that could result from over-classification of information.
- Apply identical definitions for damage levels and classification levels across the Intelligence Community and Department of Defense (DOD).

Justification Definitions

Findings

- There is no requirement for an OCA to identify or describe the damage to the national security that warrants a classification decision in a security classification guide beyond a reference to the category of national security information described by Section 1.4 of E.O. 12958, as amended. The ISOO's "Classified National Security Information Directive No. 1: Final Rule" underscores this deficiency in Section 2001.10, "Classification Standards," stating that an OCA must be *able* to support his/her decision in writing, including identifying or describing the potential damage that could result should the classification decision become the subject of a challenge or access demand.

- Not understanding the "drivers" behind classification levels complicates the comparison or combination of apparently similar information marked at different classification levels and adds subjectivity to disclosure decisions, potentially negating the sound logic behind declassification instructions. The passage of time only magnifies these difficulties.
- None of the classification guides examined by the team present clear explanation as to when or how aggregation or compilation of unclassified information becomes classified, or how the same process causes a rise from one classification level to another. This is contrary to directions set in ISOO "Classified National Security Information Directive No. 1: Final Rule," Section 2001.21, that when "the reason for classification is not apparent from the content of the information, e.g., classification by compilation, the original classification authority shall provide a more detailed explanation of the reason for classification."

Recommendations

- Establish requirements that OCAs and classification guides must provide written reasons for classifying information and that reasons such as "the information is eligible for classification according to the pertinent Executive Orders" be deemed inadequate.
- Establish a new reporting requirement for OCAs that written reasons for classifying information be categorized according to a new set of criteria. Such criteria might indicate the need to protect:
  - Content (information itself).
  - Information source(s).
  - Method of exploiting or analyzing the information.
  - Date and location that specific information was acquired.
  - Federal Government interest in a certain type of information.
  - Federal Government cognizance of or interest in information at a given time.
- Require that the written reasons for classification decisions be retained in a central policy repository and be available for use by disclosure and declassification authorities.

Intelligence Community Classification Guide Precedence

Findings

- No clarity in determining precedence of classification guides when working in inter-organizational or multi-discipline areas.
- Organizations composed of multi-agency representation or that address multi-disciplinary topics must decide on an ad hoc basis whether to write a new classification guide or to cite an existing classification guide for their classification decisions.

Recommendations

- Establish the precedence of the proposed Intelligence Community Classification Guide for issues common to multiple organizations over internally generated, agency-unique classification guides.
- Determine the appropriate approval authority for the proposed Intelligence Community Classification Guide: DNI; joint DNI and other authority such as the Secretary of Defense; or the Director of the ISOO.
- Establish policy and procedures for resolving questions about classification or requesting exceptions to guidance presented in the Intelligence Community Classification Guide.

Classification Guide Construction

Findings

- Wide dissimilarity exists in the presentation formats of classification guides. Some organizations have written their guides entirely in prose; others present general entries in table format; and yet others present detailed lists of definitions/explanations.
- Significant variance exists in the tone and style used to present guidance—from general guidelines intended to inform the user's judgment to specific encouragement to "use your best judgment" regarding "explicit rules."
- Each classification guide examined had a different method of organizing information topically.
- Among the classification guides, the use of language was inconsistent and lacked commonality (i.e., no standard lexicon).
- Only a few classification guides included an index to help the user find all the instances of a term or specific issues that might be germane to his/her particular needs.

Recommendations

- Adopt a framework for presenting and organizing topics around tasks or functions.
- Standardize presentation format and style.
- Provide cross-references to related topics or issues and use extensive mark-up and/or indexing to enhance guide usability.
- Develop a standard classification-guidance lexicon.

Classification Guide Audience

Findings

- These guides often focused on issues related to organizational functions, reflected the specific agency's culture, and/or presumed the professional education and training of the users.
- The classification guides sometimes referred their readers to other agencies' or organizations' security classification guides; however, generally that was not the case.
- The classification guides that appeared to have been written for a broader (external) audience generally focused on particular issues, systems, or projects.

Recommendations

- Develop the proposed Intelligence Classification Guide using a clear presentation format and common lexicon such that the contents will be easily and correctly understood by a wide audience.
- Develop metrics to measure and evaluate the correct interpretation of classification guidance.

Classification Duration (Declassification Dates)

Findings

- Duration of classification varies from agency to agency; information that is marked with a 10-year declassification date in one agency may be marked with a 25-year declassification date at another agency.
- Inconsistent national standards for declassification create confusion and improper implementation by users. For example, ISOO's "Classified National Security Information Directive No. 1: Final Rule" states that the OCA should attempt to determine a date or an event that is less than 10 years from the date of original classification and that coincides with the lapse of the information's national security sensitivity (Section 2001.12). Then, this directive states that if the OCA is unable to determine a date or an event of less than 10 years, a date of 10 years or up to 25 years shall ordinarily be assigned.
- Some classification guides do not require the OCA to state the original date of classification, so the original classification date of information is not readily available to derivative classifiers or declassification authorities. Consequently, dates are assigned by users based upon the date they make a derivative classification decision. Using this system, any classified product may in practical terms extend the declassification date of a particular "fact."

Recommendations

- Establish guidelines by which declassification dates may be objectively determined; publish these guidelines to the national security information community; and incorporate these guidelines *with original classification dates or events* alongside classification guidance.

Classification, Dissemination, and Handling/Release Caveats

Findings

- Several of the classification guides examined presented classification levels in columns within tables to facilitate easy comprehension by the user. In the process. many times the guides appended dissemination or handling/release caveats (e.g., NOFORN, REL TO, SCI, For Official Use Only) to classification levels (e.g., Unclassified, Confidential, Secret, Top Secret), creating the impression that different classification hierarchies and more than three classification levels exist.

Recommendations

- Separate classification and handling/release caveats in the proposed Intelligence Community Classification Guide. Ensure consistency in presentation and format.

- Thoroughly explain the common classification hierarchy in the proposed Intelligence Community Classification Guide and during user training.

National Standards for Portion Marking

Findings

- The agency classification guides inconsistently applied portion marking, as well as handling and releasability marking. Each guide exhibited different interpretations of the standards for portion marking set by ISOO and the Controlled Access Program Coordinating Office (CAPCO). This fact seemed due, in part, to the writing styles and format choices used by the developers of the guides.

Recommendations

- Present information in the proposed Intelligence Community Classification Guide in a manner that is consistent with ISOO and CAPCO standards. Furthermore, consistently apply handling, releasability, and declassification instructions to all guidance, according to current standards.

Classification Guide Location

Findings

- Intelligence Community agencies have not collected all of their classification guides in a single location that is accessible to the broader community. The CAPCO web site provides links to several key guides, but this is not a well-known fact.

Recommendations

- Determine which information is common or necessary for the broader Intelligence Community and present it in a clear, coherent manner in a central location that may be accessed by all appropriate users.
- Require that all issuers of classification guides provide to CAPCO (or other designee) a link to their guides and, if necessary, a notation that the guide is protected by a special access requirement.
- Publicize the location of the CAPCO (or other designated) web site as a source for information on diverse classification guides.

Policy Development through Technology

Findings

- Classification guidance in document format is often cumbersome and unhelpful to users

unless vigorously indexed within the guide and cross-referenced to other guides. Improving the utility of classification guides should include a facility for automated incorporation into desktop tools and decision aides. Such innovations would significantly improve usability and encourage use across Intelligence Community agency and information system lines.

- Although the compilation of a common Intelligence Community Classification Guide would simplify the question of where to turn for classification answers, it would not address the complexities of overseeing and managing thousands of classification, declassification, and disclosure policy entries nor the complexities of correlating different types of policy (e.g., classification with disclosure rules). Creation of a central or federated repository of guides, policies, and statements could draw attention to the need to consolidate the hundreds of classification guides, deconflict contradictory guidance, and enable nuanced discovery for policy implementation. This step could encourage greater transparency in the process of classifying information, as well as encourage new methods of tracking classification policies and decisions.

Recommendations

- Create a joint repository of all information policies (classification, justification, declassification, disclosure) for oversight by national policy managers.
- Determine a process for efficiently producing and maintaining classification guidance in the future.
- Create a new organizational construct for information policy management, including linkage between classification, declassification, disclosure, and information management policies in a federated or centralized repository.
- Investigate methods by which classification guidance might be employed as an enterprise solution to make available timely and authoritative information across the Intelligence Community.

CONCLUSIONS

Many Intelligence Community classification guides exist that provide methods of protecting classified information. These guides often present agency-unique and contradictory instructions that do not promote information-sharing and collaboration among the Community's agencies and mission partners. The recommendations suggested in this report constitute an essential step in strengthening the national security community. If adopted, these recommendations will immediately impact collaboration with our mission partners. As such, these recommendations will perform a vital role in implementing the Intelligence Community's "*responsibility to provide*" and assist in phasing out "*need to know*." Senior leadership must make community classification standards and policies a priority. A common understanding of the rules and reasons for classification is critical to establishing trust among the Intelligence Community and our mission partners and enabling information sharing.

Appendix A - Bibliography

Executive Order 12958, "Classified National Security Information," April 17, 1995.

Executive Order 13292, "Further Amendment to Executive Order 12958, as amended, Classified National Security Information," March 25, 2003.

"Classified National Security Information Directive No. 1: Final Rule," 32 Code of Federal Regulations (CFR), Parts 2001 and 2004, National Archives and Records Administration (NARA), Information Security Oversight Office (ISOO), September 23, 2003.

"Creating a Trusted Network for Homeland Security," Markle Foundation Task Force on National Security in the Information Age, December 2003.

Federal Information Processing Standard (FIPS) Publication (PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.

"Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment," Markle Foundation Task Force on National Security in the Information Age, July 2006.

"Protecting America's Freedom in the Information Age," Markle Foundation Task Force on National Security in the Information Age, October 2002.

"Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence," Joint Security Commission, February 28, 1994.

"Report by the Joint Security Commission II," Joint Security Commission, August 24, 1999.

"The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD): Report to the President of the United States," March 31, 2005.

"The National Intelligence Strategy of the United States of America," October 25, 2005.

"Weapons of Terror: Freeing the World of Nuclear, Biological, and Chemical Arms" Weapons of Mass Destruction (WMD) Commission, June 1, 2006.