INTELLIGENCE

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

MAY 1 9 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Fundamental Classification Guidance Review

References: (a) Executive Order 13526, "Classified National Security Information," December 29, 2009
(b) 32 Code of Federal Regulations Parts 2001 and 2003, "Classified National Security Information," June 28, 2010

References (a) and (b) require agencies to conduct a fundamental classification guidance review (FCGR) of their security classification guidance by June 27, 2012, and every 5 years thereafter. The review will ensure classification guidance reflects current circumstances (to include compliance with national classification policy) and to identify what no longer requires classification and can be declassified. It is not intended to be a superficial review but a thoughtful, methodical process using the experience and knowledge of a variety of subject matter experts.

Agency review results will be reported by the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) to the Information Security Oversight Office (ISOO) and unclassified results provided to the public. In order for the Department to meet the initial national policy deadline, we request that you have your original classification authorities (OCAs) begin this effort immediately. Agencies can obtain a listing and copies, of their security classification guides (SCG), all of which are subject to the FCGR (unless previously cancelled), by registering with the Defense Technical Information Center (DTIC) at URL: http://www.dtic.mil/dtic/announcements/DOAC.html. Unlisted SCGs (excluding drafts) should also be included in your review. For assistance, please contact [redacted].

The Department has made great strides in updating SCGs over the past three years and we strongly encourage OCAs to leverage those activities to help them accomplish this effort. Attached is a list of "Factors to Consider" while conducting the review.

OUSD(I) is required to monitor progress and we will need your plan, progress reports, and the final report in accordance with the attached milestone dates and formats. It is imperative that the Department completes this effort by the national policy deadline.

Finally, it is essential that we fulfill this requirement in a way that shows responsible stewardship of our resources. We cannot afford to expend resources on protecting information that no longer meets the criteria for classification. We appreciate each of you giving this effort your personal attention and support. The point of contact is [redacted] or [redacted].

Michael G. Vickers

Attachments:
A. Factors to Consider
B. Milestones
C. Plan Format
D. Progress Report Format
E. Final Report Format

A

DOD
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW (FCGR)
"FACTORS TO CONSIDER"

The purpose of the FCGR is to conduct a comprehensive review of each topic of security classification guidance to determine if it is still relevant to current circumstances, if it still meets the policy requirements for classification, and if there is information that can and should be declassified. Reviews shall include, at a minimum, the following regarding content and use of guidance:

- Determining if the guidance reflects current operational and technical circumstances;
- Determining if the guidance meets the standards for classification under Executive Order 13526, "Classified National Security Information," section 1.4, and using Section 1.2 of the Order, an assessment of likely damage that supports the assigned level of classification. Consideration should be given to whether information should retain its current level of classification or if it should be downgraded or declassified;
- Determining if the dissemination and availability of the guidance is appropriate, timely, and effective;
- An examination of all classification decisions that focuses on ensuring that classification decisions reflect the intent of the guidance as to what is classified, the appropriate level, the duration, and associated markings. Consideration should be given to whether the duration of classification is appropriate and, for information currently exempted from automatic declassification, whether the exemption should still apply;
- Considering whether recent original classification decisions have been incorporated in appropriate security classification guides.

Additional suggestions for components to consider include the following:

- Creation of working groups led by subject matter experts to evaluate specific topics or subject areas. Classification and declassification experts, as well as users of the guides, should be included in the working group(s).
- Contributions of subject matter experts with sufficient expertise in narrow specializations must be balanced by the participation of managers and planners who have broader organizational vision and relationships.
- Past declassification decisions (under automatic declassification as well as those made in response to Freedom of Information Act and Mandatory Declassification Review requests, and by the Interagency Security Classification Appeals Panel) should be reflected in updated classification/declassification guidance.

Attachment 1

- Agencies should be specific in their determinations as to what no longer requires protection. An example would be a specific part of a weapon system versus the weapon system as a whole. The user of the guide must be able to identify the specific element of information that does or does not require protection.

- Cross-reference information with other guides, both within and outside your agency. Is it possible that information in your guides is also in other organizations' or agencies' guides? If so, are the instructions the same? If there is a difference, is the distinction readily known and apparent? Do the guides contain cross-referenced information?

B

DOD
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
"MILESTONES"

Action	Milestone Date
USD(I) Initiates DoD FCGR	April 2011
DoD Component FCGR Plan to USD(I)	May 5, 2011
DoD Component Progress Report to USD(I)	July 6, 2011
USD(I) Progress Report to SecDef	July 15, 2011
USD(I) Progress Report to ISOO	July 29, 2011
DoD Component Progress Report to USD(I)	October 6, 2011
USD(I) Progress Report to SecDef	October 15, 2011
DoD Component Progress Report to USD(I)	January 6, 2012
USD(I) Progress Report to SecDef	January 16, 2012
USD(I) Progress Report to ISOO	January 31, 2012
DoD Component Final Report to USD(I)	March 9, 2012
USD(I) Final Report to ISOO	June 27, 2012
USD(I) Final Report to Public—Unclassified version approved for public release	June 27, 2012

DoD Component plan, progress reports and final report must be signed by the Component Senior Agency Official or designated representative.

Attachment 2

C

DOD
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
"DOD COMPONENT PLAN"

Date:

DoD Component:

POC/Phone/Email:

Introduction/Purpose:

DoD Component Mission Summary and Organizational Structure:

Scope: Provide number of security classification guides (SCG) produced by the component and any other information necessary to understand the scope of this effort.

Plan: Describe the plan for completing the component fundamental classification guidance review (FCGR). Include a description of the planned approach as well as internal milestones or schedule for completing the reviews and reporting requirements identified by USD(I).

Attachment 3

D

DOD
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
"PROGRESS REPORT FORMAT"

Date:

Component:

POC/Phone/Email address:

Progress Update:

- Total number of SCGs:________
- Total number of SCGs for which a FCGR has been initiated:________
- Total number of SCGs for which a FCGR has not been initiated:________
- Total number of SCGs for which a FCGR has been completed:________
- Total number of SCGs to be eliminated:________
- Annotate status of each security classification guide (SCG) on the component list of SCGs using one of the appropriate status statements provided below:

  a. When a FCGR has been initiated, annotate the applicable SCG line with: "Initiated (Date)/Estimated Completion Date (ECD): (Date)"

  b. When a FCGR has *not* been initiated, annotate the applicable SCG line with: "Estimated Initiation Date (EID): (Date)/ECD: (Date)"

  c. When a FCGR has been completed, annotate the applicable SCG line with: "FCGR: (Date completed)." If the SCG will be eliminated, add the additional annotation: "(Eliminate)."

E

DOD
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
"FINAL REPORT FORMAT"

Date:

Component:

POC/Phone/Email address:

Report. Each DoD component will provide a consolidated report to USD(I) providing the following information:

- Provide a brief summary of primary topics of information classified by your component.

- Total number of SCGs for which a FCGR has been completed:________.

- Total number of SCGs eliminated as a result of the FCGR:________. Identify the reason for elimination, e.g., consolidated or integrated into other SCGs, information declassified, etc.

- Certify that your component's SCGs are compliant with security classification policy and updates have been provided to DTIC with the applicable DD Form 2024, DoD Security Classification Guide Data Elements.

- Explain the overall FCGR approach, e.g., working group method, composition of working group, etc.

- Provide annotated list of SCGs to show when the FCGR was completed for each SCG and include it as an attachment to report.

- Summarize for each SCG what information was declassified as a result of the FCGR. Indicate if the summary is releasable to the public in accordance with a security review. Indicate if the declassified information has been released to the public. If so, identify through what means and provide the public website address, if applicable.

- Share best practices and identify lessons learned from the experience.

Attachment 5