U.S. DEPARTMENT OF ENERGY

National Security Information Fundamental Classification Guidance Review

Report to the Information Security Oversight Office
June 2012

United States Department of Energy
Washington, DC 20585

Message from the Senior Agency Official

I am pleased to forward the Department of Energy's National Security Information (NSI) Fundamental Classification Guidance Review report. The Department has endeavored to provide as much unclassified information as possible in this report to demonstrate our commitment to the democratic principle that the American people be informed of the activities of their Government. Every recommendation in this report presents an opportunity for improvement in our NSI classification guidance. Those recommendations the Department implements, in revisions to classification guides, will result in better derivative classification and declassification decisions, and decrease unintentional overclassification. This report will be posted on my Department's web site.

We appreciate the opportunity to further the President's goals for greater openness while protecting legitimate national security interests. If you have any questions or need additional information, please contact Edith Chalk, Director, Office of Technical Guidance within the Office of Classification, at (301) 903-3521.

Sincerely,

W. a. Eckroade

William A. Eckroade
Principal Deputy Chief for Mission
Support Operations
Office of Health, Safety and Security

Executive Summary

Section 1.9 of Executive Order (E.O.) 13526, *Classified National Security Information*, dated December 29, 2009, directs agency heads to complete a comprehensive review of agency classification guides to ensure they reflect current circumstances and to identify classified information that no longer requires protection and can be declassified. To meet this requirement, the Department of Energy (DOE), under the direction of the Senior Agency Official, devoted 2½ years to reviewing the DOE classification program. In this review, DOE assessed and evaluated the technical content of all National Security Information (NSI) classification guidance.

The DOE Office of Classification evaluated 67 Headquarters (HQ) classification guides and 11 HQ classification bulletins to identify over 2,800 NSI topics. Thirty-six subject area working groups then examined these NSI topics, using almost 200 subject matter experts (SMEs). These SMEs, from across the nuclear weapon complex and other partnering agencies, identified the essential information protected through classification, explained why the information requires continued classification, and recommended improvements to the existing classification guidance. A Steering Committee of senior classification experts reviewed the recommendations of each working group to maintain consistency and balance throughout the process.

In addition to determining which NSI requires continued protection and which may be declassified, DOE has identified significant improvements that will streamline the NSI classification guidance. These improvements include: canceling unnecessary guides, deleting redundant topics, clarifying ambiguous topics, reducing the number of topics exempting information from automatic declassification, and replacing subjective or hard-to-determine declassification events with fixed durations of time until declassification.

Because of this rigorous review, DOE has identified many areas where classification guidance can be consolidated, eliminated, or clarified to address concerns identified in E.O. 13526 and in many other studies regarding the Government's use of classification. Clear, concise guidance will significantly reduce the potential for Derivative Classifiers to misinterpret the intent of classification guide topics that can result in underclassification and overclassification of information.

The Report's recommendations, if fully carried out, will result in:

- A 33 percent overall reduction of NSI classification guide topics
- A 42 percent reduction in topics with exemptions from automatic declassification
- A 52 percent reduction in the use of topics with event-based declassifications
- Twenty-two declassification actions primarily related to physical security, transportation, and materials
- Cancellation of 18 classification guides and 9 classification bulletins

Implementation of these recommendations will dramatically improve the clarity and accuracy of existing classification guide topics and will result in fewer instances of underclassification and overclassification while improving the protection given to information truly requiring it.

As a natural consequence of conducting the Fundamental Classification Guidance Review (FCGR), DOE has also revised CG-HR-3, *Historical Records Declassification Guide,* which will serve to implement the recommendations from the FCGR concerning the duration of classification. The revised guide, CG-HR-4, provides updated guidance for DOE Derivative Declassifiers conducting systematic reviews of historical record collections for possible declassification and identifies information exempt from automatic declassification at 25 and 50 years.

National Security Information Fundamental Classification Guidance Review

Contents

I. Introduction 1
II. Methodology/Process 3
III. Execution 6
IV. Reporting 8
V. Results 9
A. Working Group Recommendations 9
1. Examples of Recommendations to Address Broad/Vague Topics 10
2. Examples of Recommendations to Address Other Agency Determinations in DOE Guidance 12
B. Overall Recommendations 14
VI. Summary 16
VII. Appendices 19
Appendix A. Electronic Publishing Tools 20
Appendix B. National Security Information Fundamental Classification Guidance Review charter dated November 4, 2010 23
Appendix C. Thirty-six subject areas 32
Appendix D. DOE steering committee members 35
Appendix E. DOE action/outcome chart 37
Appendix F. DOE steering committee schedule 40
Appendix G. DOE reasons for classification chart 42
Appendix H. DOE steering committee reporting chart 44
Appendix I. Thirty-six working group reports 48
Appendix J. List of DOE keystones 154
Appendix K. Summary of DOE 50-year exemption memorandum to the Information Security Oversight Office 157
Appendix L. List of Acronyms and Abbreviations 160

Figures

Figure 1. FCGR Process 5
Figure 2. Initial Guidance Conditions 9
Figure 3. Recommended Guidance Conditions 16

I. Introduction

> "Developing a sound policy on the classification of information requires the balancing of overlapping and competing considerations: protecting national security, encouraging an informed citizenry and a knowledgeable group of policymakers in Congress and the executive branch, facilitating the achievement of departmental missions, encouraging fiscal efficiency, assuring the effectiveness of the classification system, and weighing the international implications of DOE policy."

These words could have been taken from any number of recently issued studies, such as the Brennan Center for Justice report, dated October 2011, *Reducing Overclassification through Accountability*, or the report *Improving Declassification*, from the Public Interest Declassification Board, dated December 2007, but they were written by the Openness Advisory Panel to the Secretary of Energy in 1997. They concerned the Fundamental Classification Policy Review that was conducted by the Department of Energy (DOE) in 1995 and 1996. That review of classification policy resulted in many concrete proposals for the declassification of information and serves as an example that the periodic review of classification guidance is essential to ensuring that only truly sensitive information is protected through classification.

The DOE Office of Classification (OC) within the Office of Health, Safety and Security (HSS) relies on a hierarchy of classification guides and authorities to promulgate DOE classification policy. Classification guides are the instruments used by authorized individuals to derivatively classify and declassify information to ensure consistent and accurate classification determinations throughout the Department. In addition, classification guides are centrally approved by OC to ensure like information is classified at the same level and for the same duration of time. Finally, DOE policy limits who has authority to use guides to classify and declassify documents through a structured process of specific training, testing, and certification in order to ensure that guidance is correctly interpreted.

In DOE, an original classification authority (OCA) provides the initial determination that release of a specific piece of information pertaining to at least one of eight allowed categories of Executive Order (E.O.) 13526, *Classified National Security Information*, dated December 29, 2009, would result in damage to national security.[1, 2] An OCA also establishes the date or event for the declassification of the information.[3] These original classification determinations are recorded in classification guides or classification bulletins for use by classifiers and declassifiers throughout the Department. Due to the extensive collection of classification guidance that is in place, DOE currently has only 13 OCAs and makes very few original determinations in any year. Historically, the Director, OC has made a majority of the original decisions for DOE by signing classification guides.

Most of the Headquarters (HQ) classification guides contain topics that classify information as Restricted Data (RD) and Formerly Restricted Data (FRD) under the Atomic Energy Act of

[1] E.O. 13526 Section 1.1(4)
[2] E.O. 13526 Section 1.4
[3] E.O. 13526 Section 1.5

1954, as amended. Because this information is exempt from disclosure under statute and is not classified, downgraded, declassified, handled, or protected under E.O. 13526, these topics are outside the scope of this review. Approximately 2,800 guide topics dispersed throughout 67 classification guides and 11 classification bulletins classify National Security Information (NSI) per E.O. 13526 and are subject to the Fundamental Classification Guidance Review (FCGR).

In practice, a Derivative Classifier (DC), acting within his or her designated authority and subject area competence, determines if information in documents is, in substance, the same as information that has been originally classified and captured in classification guides or source documents.[4] The DC then marks the document or directs the document to be marked in accordance with the decision derived from the guidance. While DOE permits the use of source documents for derivative classification determinations, such documents may only be used in limited circumstances.[5] This reflects the DOE perspective that classification guides are superior to source documents in terms of accuracy of the classification determination. It is imperative, therefore, that classification guidance covers all needed NSI subject areas and that the topics are clear and concise. This allows the DC to make an accurate classification determination.

It is also DOE policy to have specifically trained individuals called Derivative Declassifiers (DDs) determine whether a currently classified document or material may be declassified or downgraded in classification level. DOE uses DDs because of the additional knowledge and skills needed beyond those of a DC in order to accurately redact, downgrade, or declassify a classified document. Because DDs use classification guides to make these decisions, it is important that guidance is clear so DDs can declassify documents in an accurate and consistent manner.[6]

As DOE conducts classified activities and research in a variety of technical areas, many unique classification guides have been developed for specific programs over the years. Many of these specific program guides repeat topics found in other guides to allow each guide to be a stand-alone document. DOE maintains approximately 100 HQ classification guides for use throughout the DOE/National Nuclear Security Administration (NNSA) complex. HQ classification guides also serve as the basis for the determinations in approximately 80 local classification guides that tailor the topics in HQ guides to apply to unique information at a given field site.

Over the years, it has been difficult to identify all the occurrences of the same guide topic throughout all of the guides when changes occurred. The resultant inconsistencies in wording, classification levels, and declassification instructions of similar or identical topics increase the likelihood for confusion and inconsistent application of the guidance. Over two decades ago, DOE OC began investing in automation tools to improve the process to author and maintain classification guides (Appendix A). Specialized software now allows classification guides to be created, maintained, and published electronically. This software also has the ability to link related guide topics together and record their underlying reasons for classification. This capability assists guide authors in identifying all occurrences of a topic and concept throughout DOE guidance, ensuring guidance consistency and that any classification changes are reflected

[4] E.O. 13526 Section 2.1(a)
[5] DOE O 475.2a, Attachment 4 1.b.(3)
[6] DOE O 475.2a, Attachment 4 2.b.

in all affected topics. A major strength of DOE's centralized, digitized approach to authoring, approval, publication, and distribution of classification guidance is that similar information is classified in a consistent manner across DOE.

DOE routinely evaluates the use and availability of its classification guidance to determine whether access to guidance is appropriate, timely, and effective. Based on these ongoing evaluations, OC established a push/pull system to certify that DCs and DDs receive the guidance they need. OC maintains an electronic distribution system to distribute guides, as appropriate.[7] OC also publishes a biannual index of classification guides so DCs and DDs can verify they have the proper versions of the guides and request copies as needed. Twice a year, OC updates the electronic Classification Guidance System (eCGS), a searchable electronic database of active and cancelled guides and bulletins. To reduce both printing and mailing costs, OC is currently distributing all unclassified classification guidance electronically. OC plans to distribute classified guidance electronically once the infrastructure is in place. These tools allow DOE to distribute any new or updated classification guidance to the individuals who require it in a timely manner.[8] The availability of current classification guides to DCs and DDs is an area that is assessed during DOE's classification program evaluations.

II. Methodology/Process

On November 4, 2010, Edith Chalk, Director, Office of Technical Guidance within OC, signed a charter (Appendix B) establishing the FCGR process for DOE. The goals of this process were to evaluate the guidance content, determine if the guidance conforms to current operational and technical circumstances, determine if the guidance meets the standards for classification under section 1.4 of E.O. 13526, and assess the likelihood of damage under section 1.2 of E.O. 13526. This process contained eight steps, which are summarized in Figure 1:

1. Preparation of Classification Guidance Topics for Review - OC reviewed current classification guidance to identify all 2,800+ NSI topics. These were then categorized into 1 of 36 subject areas listed in Appendix C. Inside each of these subject areas, the topics were grouped by common declassification instructions.

2. Steering Committee Actions - Senior management appointed senior DOE/NNSA classification experts from the major DOE program offices to the Steering Committee. These individuals were selected to provide a broad range of perspectives throughout the execution of the FCGR. The Steering Committee reviewed, analyzed, and critiqued all of the working group recommendations to maintain consistency of the final working group product. Appendix D identifies the Steering Committee members.

3. Formation of Subject Area Working Groups - Thirty-six working groups were formed to engage approximately 200 subject matter experts to review and analyze NSI guidance topics and to make recommendations for improvements.

[7] 32CFR2001.16 (b)(1) and (b)(2)(i)
[8] 32CFR2001.16(b)(2)(i)

4. Operating Principles of Subject Area Working Groups - Each working group assessed topics in its subject area against the requirements identified in E.O. 13526. These principles are discussed in the next section of this report. The nine-step evaluation process followed by each working group is contained in Appendix E.

5. Subject Area Working Group Logistics - Working groups that were addressing complex classification issues or that involved other agency coordination required more time than those that reviewed only a few topics. Working groups met directly or through videoconference, and corresponded by e-mail. These factors drove the overall working group schedule to brief the Steering Committee (Appendix F).

6. Review of Other Agency Equities - The working groups identified a significant number of topics as equities belonging to Other Government Agencies (OGAs) or equities held jointly between DOE/NNSA and an OGA. For equities belonging to OGAs, the detailed topics and background information were transmitted to the owning agency. The working group reviewed joint equity topics.

7. Compilation and Reporting to the Information Security Oversight Office (ISOO) - Working group progress was monitored and reported on a weekly basis to the DOE Senior Agency Official and on a semi-annual basis to ISOO.

8. Classification Guidance Revision - Based on working group results and as reviewed by the Steering Committee, recommendations have been and continue to be routed through OC, DOE/NNSA program offices and, where applicable, OGA officials in order to revise relevant classification guidance.

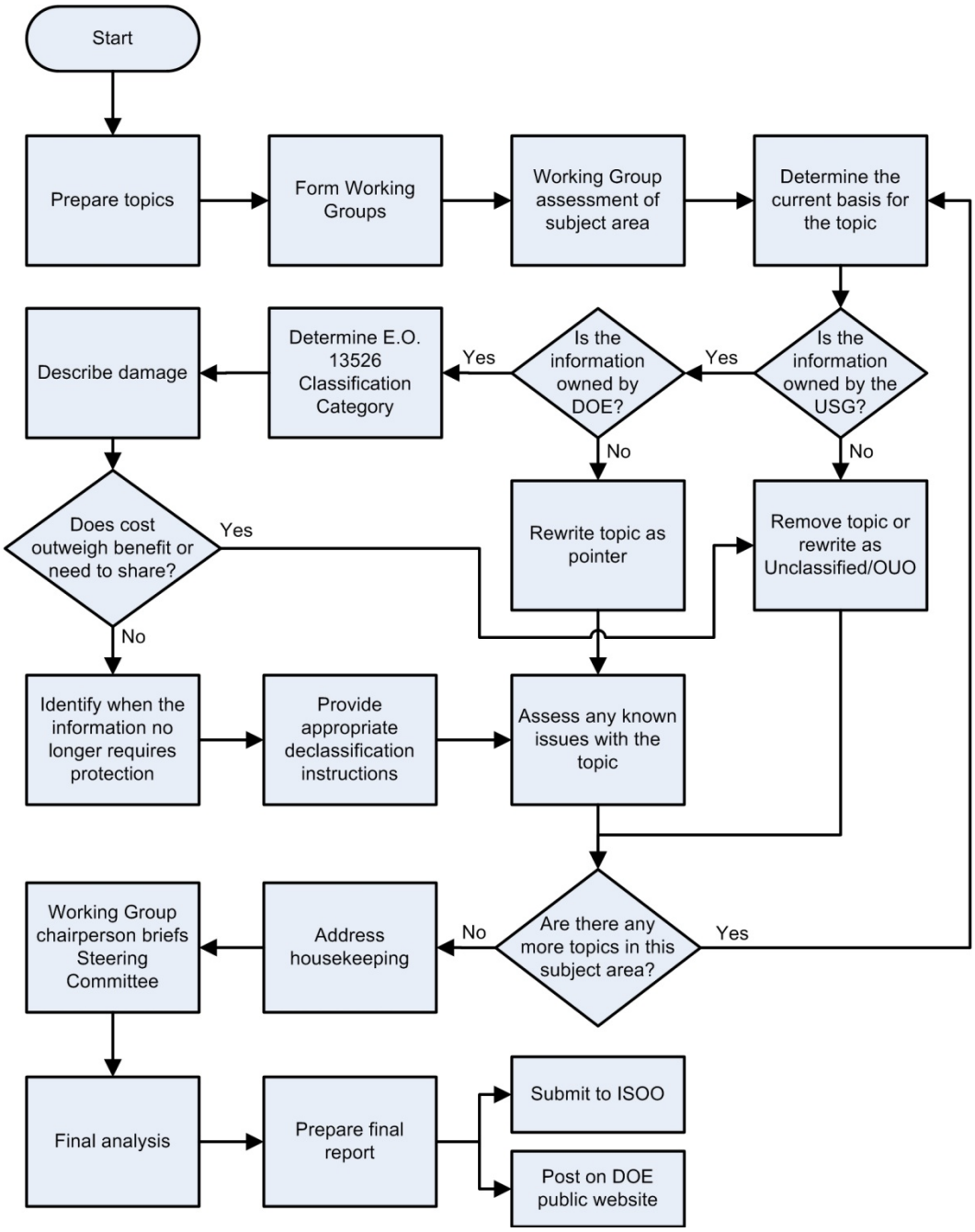


Figure 1. FCGR Process

After determining that a piece of information met the standards for classification under section 1.4 of E.O. 13526 and assessing the likely damage under section 1.2 of E.O. 13526, each working group determined the basic essential information that required protection through classification. Defining these key concepts, or keystones, ensures guide topics accurately protect the appropriate NSI. The working groups verified each topic had a clearly defined basis for classification, described the damage to national security, and provided appropriate

declassification instructions. When declassification instructions were event driven, the working groups verified that the events were clearly described or a declassification date was assigned.

III. Execution

In January 2010, DOE OC began reviewing classification guides under the FCGR to identify all NSI topics. Ultimately, over 2,800 NSI topics were identified and examined to determine the appropriateness of the classification level, duration, and associated details. Topics in a common subject area were grouped together (not necessarily by classification guide) into 36 unique subject areas. OC identified members for the 36 working groups that analyzed the topics in each of these subject areas. To provide a broad range of perspectives, the working group membership included experts in classification and experts in the relevant subject matter from both Headquarters and field locations. Working group activities identified in DOE's FCGR Charter began in November 2010.

OC charged each working group to review and assess multiple characteristics of guidance topics. Some of these common review objectives were requirements of E.O. 13526, and some were to improve the quality of the DOE classification guidance. These review objectives were:

Assess whether the information is owned by, produced by or for, or is under the control of the United States Government (USG).[9] This includes determining whether DOE or another USG agency owns the information. This assessment allowed the working group to determine that the information was indeed owned by the USG and to identify the "owning agency" of the information equity. If the agency was other than DOE and the guide was not a joint guide (i.e., signed by DOE and the other agency), then the topic was marked for referral to that agency. If a topic was a joint equity or solely a DOE equity, the working group continued the analysis process for that topic.

Determine the current basis for the topic. A basis topic conveys a specific original decision by an OCA. In this decision, the OCA is classifying a key concept or keystone. Topics dependent on a basis topic identify specific ways the information classified by the basis topic can be revealed. For example, multiple material transport topics (e.g., schedules, routes) are based on classifying information that reveals the current location of a shipment. When a clear basis topic was identified for a "dependent" topic, the working group documented the relationship. Also, the working group identified the keystone being protected by the topic.[10] Information developed from this step will be added as the "basis link" and "keystone" in the metadata for that topic when guidance is revised.[11]

Verify the E.O. 13526 Classification Categories[12] by which the information is classified. If the information classified by the topic did not fall into the approved classification category, then it could not be classified as NSI unless a valid category could be determined by the

[9] E.O. 13526, Section 1.1 (2)
[10] See previous section for discussion of keystones.
[11] See Appendix A.
[12] E.O. 13526, Section 1.4 (a) – (h)

working group that would then be approved by an OCA. The chart in Appendix G was used as an aid to standardize the process.

Identify/describe the damage to national security that would result from the unauthorized disclosure of the information protected by this topic. The working group analyzed and provided a basis for the classification level or range of classification levels for each topic.[13] If a topic had a range of classification levels, then the working group identified the discrete differences between the classification levels. When dependent topics were identified, the classification level normally agreed with the level and duration of the basis topic. For cases where the classification of the dependent topic varied from its basis, the working group provided justification as to why this was not a new classification decision.

Based on the identifiable damage to national security, determine if the need to share the information or the cost of continuing to protect the information outweighs the benefit of protection. If the working group determined national security would be better served by sharing the information rather than limiting it to cleared individuals, the information would not be classified. Likewise, if the working group determined that the potential damage to national security did not rise to the level that required the expenditure of our limited resources to protect it, then a lower classification level or a declassification was considered.

Identify when the information no longer requires protection. The working group determined either a specific duration or a specific event when the information would no longer cause damage to national security. The working group was required to justify why declassification of information at or before 25 years would cause damage to national security. If it was determined that disclosure of the information 25 years or more after its creation would still cause damage to national security, the working group identified the appropriate exemption code for the information.[14] In these cases, the working group also recommended CG-HR-3, *Historical Records Declassification Guide*, be updated to record any changes to exempt information.

Provide accurate declassification instructions. For events, the working groups needed to provide instructions that a DD reviewing documents could understand and apply. In many cases, DDs involved in review of decades old documents have limited programmatic expertise, particularly for collections associated with programs long since concluded. Because of this, declassification instructions need to provide clear, easily verified conditions for declassification. The working groups also addressed other issues with declassification events, such as referral to other agencies for declassification instructions. For topics such as these, the information being protected was analyzed to determine if there was a DOE equity. If not, the topic was replaced with instructions to contact the other agency for classification guidance.

Assess any known issues with the accuracy and availability of the topic. The working groups, which consisted of both classification and subject matter experts, reviewed the topics to ensure their technical accuracy and to verify that the terminology and structure of the

[13] E.O. 13526 Section 1.2
[14] E.O. 13526 Section 3.3(b)

topics agreed with current programmatic, operational, and technical standards. The working group members determined if the intent of the guidance as written was being followed or if clarification was required.

Review any known issues regarding the application of a topic by DCs. OC also identified topics that would benefit from restructure or rewrite. These modifications included: restructuring topics that attempted to classify multiple pieces of information as several individual topics, removing classification levels and categories from topics that had nested topics with their own level and category determinations, rewriting topics in clear and concise language, and better defining when a particular classification level applied to a topic with a range of classification levels.

The Steering Committee met on 11 occasions (as outlined in Appendix F) to review each working group's findings and recommendations, which were standardized for presentation on a Steering Committee Reporting Form (a blank form is included as Appendix H**)**. The Steering Committee provided oversight and guidance that maintained consistency throughout the process. The 36 working groups used this feedback to prepare their final working group reports.

The Office of Technical Guidance compiled the working group recommendations to exempt information from automatic declassification at 25 years and incorporated them into CG-HR-4, the CG-HR-3 replacement.

IV. Reporting

The 36 working group reports contained 4 sections: Current Policy, Background, Analysis, and Recommendations (Appendix I).[15]

The Current Policy section discusses why classification guidance in a given subject area is necessary. This section contains a description of the subject area and a brief summary of the classification guidance.

The Background section lists the number of topics in the subject area, grouping them according to declassification instructions. Topics that point to guidance subject to review by a different working group were identified, as well as topics that use guidance from other agencies as their basis. For most topics exempt from automatic declassification at 25 years, this section also identifies the current exemption code for the information.

The Analysis section identifies any keystones, discusses why they require classification, and describes the ways the information identified by the keystones could be revealed. This section specifies any classification durations or declassification events for the information. Finally, it identifies any information that is the equity of another agency.

The Recommendations section describes how application of the working group determinations would affect guidance. This includes any discussion of changes in the total number of topics, the

[15] Classified reports have been rewritten as unclassified documents. Classified working group reports will be provided separately.

exemption codes in use, and the cancellation of any guides. This section also identifies the impact of the changes for use by the Director, OC.

V. Results

Prior to analysis by the working groups, OC reviewed current classification guidance to identify all 2,800+ NSI topics. These were then categorized into 36 subject areas. Inside each of these subject areas, the topics were grouped by common declassification instructions. Figure 2 summarizes the initial classification guide conditions.

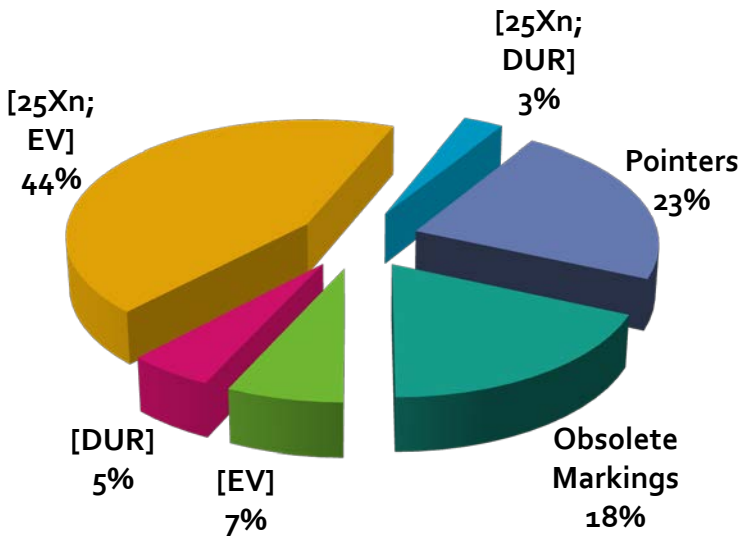


Figure 2. Initial Guidance Conditions[16, 17]

A. Working Group Recommendations

The working groups' analyses produced over 100 recommendations. Some of these recommendations responded to unique issues identified by the working groups for their subject areas. Other recommendations, independent of one another, identified issues found throughout DOE guidance. The following paragraphs provide examples of these common issues. The working group reports (Appendix I) describe all the recommendations, the underlying issues that led to them, and the impact of their implementation.

[16] See List of Acronyms and Abbreviations (Appendix L) for a description of terms.
[17] Obsolete markings refer to markings approved under previous Executive orders, but not in conformance with the approved markings in E.O. 13526.

1. Examples of Recommendations to Address Broad/Vague Topics

DOE structures its classification program to rely on DCs using classification guides to make determinations rather than OCAs making a large number of original classification decisions. As DOE consists of a large number of contractors relative to Federal staff and an original classification decision is an inherently Federal function, this structure is appropriate. However, there are some instances where guide topics cannot clearly constrain the information requiring classification. These topics provide broad or vague instructions that can be problematic for the DC or DD to interpret. This increases the probability of underclassification or overclassification. The following five examples from different working groups illustrate methods of reducing inconsistency in derivative classification:

Eliminate pointer topics in DOE safeguards and security guidance.

In current DOE safeguards and security guidance, many topics are based on a much smaller set of topics that, while not identified as such, function as classification keystones. For example, dozens of topics for physical security components base classification on or direct the DC or DD to only a few vulnerability and method/technique topics. Most or all of the "pointer" topics can be eliminated without any loss in guide functionality, leaving only the few basis topics. In fact, this would improve guide clarity and usability.

Cancel current general derivative classification guidance for non-Office of Secure Transportation (OST) inter-site shipments of Category I/II Special Nuclear Material (SNM).

Any future non-OST shipment should be examined on its particulars to identify what can and should be classified. Because DOE regularly ships SNM through OST, most DOE employees involved in those shipments possess a general understanding of what information about an upcoming OST shipment is classified and control it accordingly. A similar understanding does not exist for non-OST shipments, leading to less awareness of what information is classified. Future non-OST shipments may have unique information that cannot be controlled as classified as well. For example, the amount of material being shipped from one site to another in a shipment may have been announced as a consolidation of material at the receiving site. The route used by another shipment may require disclosure of some of details of the shipment to state or local law enforcement. Because each shipment may have different information about it that cannot be controlled as classified, broad topics will not properly protect information that will allow for the derivation of sensitive information about the shipment. Rather than using the current broad topics, the information both publicly available and controlled as OUO (or UCNI) for a shipment should be examined to determine what information such as the timing, route, and contents for a specific trip can and should be protected through classification. An OCA designated for the site's or program's safeguards and security information can then make a determination to

classify shipment/site specific information, and guidance will be generated accordingly.

Require the policy office to maintain an adversary capabilities list with each specific adversary capability uniformly classified with the newly identified graded security protection (GSP) adversary capabilities keystones.

For GSP guidance, many of the topics were not specific enough for a DC or DD to apply to the specific, detailed descriptions of adversary characteristics and capabilities now found in the GSP policy. To clarify the intent of the topics, the basic "keystones" for GSP information were identified. The keystones were used to identify the types of capabilities that would require classification. The policy office responsible for the GSP is the only organization knowledgeable enough to determine which adversary capabilities require protection under these keystones.

Remove derivative classification determinations for critical infrastructure information (CII) from DOE classification guidance.

To apply the existing CII topics, a DC must make a subjective determination that the information impacts national security. As this determination should be reserved for an OCA, these topics should be removed from guidance. If DOE identifies information in this subject area that requires classification, an OCA will classify that specific information and guidance will be generated to document the decision.

Grant additional original classification authorities to key personnel in intelligence and counterintelligence.

In DOE, the intelligence and counterintelligence functions are consolidated into one organization called the Office of Intelligence (IN). The topics in the existing guidance contain broad instructions that have proven difficult for DCs to apply consistently. For example, the following topic is very difficult for a DC to apply:

> "Information that reveals, or tends to reveal, specific U.S. policy interests, options, concerns, or considerations that, if released, could negatively impact the conduct of U.S. foreign policy."

The vagueness of this type of guidance topic forces the DC to make a subjective determination as to how the release of the information would cause damage to national security. These types of decisions are best left to an OCA.

In addition, the information addressed by these types of topics often contain equities of other agencies in the intelligence community (IC). For example, a large amount of counterintelligence (CI) information, particularly when associated with investigations and inquiries, is a joint equity with the Federal Bureau of Investigation (FBI). As many of the classification and declassification decisions are, by necessity, case specific, rather than depending on a DC to make difficult determinations about

ownership of the information and damage caused to national security by its release, a DOE OCA should classify this information. This original determination will then be documented in new derivative guidance for that specific case.

2. Examples of Recommendations to Address Other Agency Determinations in DOE Guidance

In the past, DOE included guidance topics that reflected the classification determinations of other agencies to assist DCs in making classification determinations for DOE programs that may involve these other agencies' equities. With the passage of time, these topics lost their explicit connection to the other agency and appeared to be protecting DOE equities. This resulted in a situation where DCs could be making erroneous classification determinations for information not owned by DOE. Several working groups have recommended removing these types of guidance topics and referring the information to the other agency for a classification determination. The owning agency for the equity will have the most current classification guidance for the equity because the FCGR requires all agencies with classification authority to identify the correct classification level and duration for their information, both now and at least once every five years thereafter.[18] The following five examples from different working groups recommend referring information to other agencies for guidance:

Remove the TEMPEST, COMSEC, and Cryptology Information topics from DOE classification guidance.

The Atomic Energy Commission (AEC), a predecessor agency to DOE, participated in the pilot program for the implementation of Secure Terminal Equipment (STE) in the Government. During this pilot, the AEC OC raised questions about the classification of information related to this program. The AEC provided the National Security Agency (NSA), the owners of the STE information, with recommendations as to what would require classification about the program. NSA concurred with these recommendations, and AEC issued a classification guide. Over time, the connection of this guidance to the NSA lost fidelity. By 1994, the guidance was no longer being sent to NSA for concurrence. These topics were provided to NSA, the equity owner for COMSEC information, as reference for its FCGR activities. NSA determined that this DOE guidance was no longer needed as NSA has made its guidance more widely available.

Delete all 37 safeguards and security-related topics, originally inserted at the request of the Nuclear Regulatory Commission (NRC) from CG-PGD-5, the *Joint NRC/DOE Classification Guide for Uranium Isotope Separation by the Gaseous Diffusion Process*, and re-issue the guide as a DOE only guide.

This guide contains 37 topics that point to topics in either the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4) or NRC guidance.

[18] 32CFR2001(a)

DCs at the United States Enrichment Corporation (USEC) indicated they use the topics in CG-PGD-5 rather than in CG-SS-4. After a review of the topics in CG-PGD-5 by DOE and NRC, it was determined that topics in CG-SS-4 would adequately protect the information classified by the safeguards and security topics currently in CG-PGD-5. As a result, these 37 topics can be removed from CG-PGD-5, and DCs will use CG-SS-4 to make classification determinations for gaseous diffusion related safeguards and security information.

Remove classification and declassification instructions for other agency information from IN/CI classification guides.

Many of the topics for both IN and CI provide instructions for other IC agency equities so they are recommended for deletion. Most of the CI topics address information for which DOE shares equity with other IC agencies or organizations, primarily FBI. None of these IN/CI classification guides are joint guides. Because these are DOE only guides, information that is solely classified by another IC agency should not be classified by DOE topical guidance. Concerns about other agency classified information are better addressed in notes or cautions to topics.

DOE will assist the Department of Homeland Security (DHS) to develop a DHS only classification guide for activities and detection systems related to nuclear smuggling. Upon completion of the DHS guide, DOE will cancel CG-SMG-2, the *Joint CBP/DOE Classification Guide for Nuclear Smuggling Information*.

The DOE does not have a nuclear smuggling program, although several National Laboratories conduct activities in support of DHS. The current guidance was developed as a joint guide with DHS Customs and Border Protection (CBP) because, at the time of development, the DHS did not have the infrastructure in place to develop, produce, and distribute the guide. This guide was provided to the now established DHS Classification Office to determine if it is still needed. The NNSA Office of Emergency Response (NA-42) also reviewed the guide. After review, it was confirmed that all classification determinations are derived from topics in other DOE classification guides or DHS classification guides. Because these other guides provide adequate guidance for DOE but not DHS, CG-SMG-2 will be converted to a DHS classification guide.

Delete 30 topics concerning the Strategic Defense Initiative that relate to information that has been declassified by the Department of Defense (DoD).

In this subject area, 30 topics cover space reactor power system military requirements and applications. These topics originate in some uses for space reactors envisioned as part of the Strategic Defense Initiative of the 1980s. The superseding agency, the Missile Defense Agency, determined that this is its equity and no longer requires protection and should be declassified.

B. Overall Recommendations

One major improvement made possible by the FCGR is the identification of classification keystones for the NSI topics. Prior to the FCGR, keystones were not identified for the NSI topics in DOE classification guidance. This often caused ambiguity with what the topic was attempting to protect. Defining the keystones allows for the identification of the underlying information that requires protection in accurate classification guidance.

Some keystones are expressed as unique guide topics. Other keystones, due to the conditional limitations on their application, are not expressed as unique topics because the resulting topics would be too vague for application by a DC. For example, the keystone "information that assists an adversary in acquiring SNM", if expressed as a topic, would require the DC to determine if a piece of information does assist an adversary. Because this determination is outside the scope of a DC's authority, guide topics for these types of keystones are developed with the assistance of security experts who can determine whether a specific piece of information does assist an adversary. A DC can then classify information dependant on these keystones because the conditional determinations have been made. This does, however, result in more topics than keystones.

The FCGR working groups identified 77 unique keystones (see Appendix J for a list). As noted in the Brennan Center for Justice Report, *Reducing Overclassification Through Accountability*, overly broad topics rely very heavily on the discretion of the DC. Identifying the keystones allows the classification guidance to contain topics that are more specific. This reduces the subjectivity in the application of the classification guidance and facilitates uniform classification determinations.

There were also several inconsistencies in classification level and classification duration for topics that protected the same information. The identification of keystones allowed for the deletion of slightly less than 30 percent of the topics because they were either duplicative of other topics, or they did not address their identified keystone as well as a smaller number of recommended replacement topics. Twenty-two topics were identified for declassification because the related keystone no longer applied to the information classified by these topics.

Adopting all the recommendations would reduce the number of topics exempt from automatic declassification by more than 40 percent. The number of topics with an event-based declassification, including those exempt from automatic declassification, would be reduced by slightly more than half. The number of topics with a specific duration for classification (e.g., 25 or 50 years) would decrease by approximately 6 percent. This smaller decrease can be attributed to a recommended shift from event-based declassifications to specific classification durations. Specific classification durations provide definitive instructions for DDs as to when classified information would no longer cause damage to national security.

DOE identified the need to apply a 50-year exemption for key design concepts of weapons of mass destruction (WMD) that were not protected as RD or Transclassified Foreign Nuclear Information. Slightly more than seven percent of the topics exempt information from

automatic declassification at 50 years because the information protected by these topics reveal key design concepts for WMDs that would assist in the development, production, or use of a WMD. The majority of these topics address security systems for nuclear weapons that were designed in the early 1970s with design documentation that would be over 50 years old by 2020. Access to this design information would impair the effectiveness of the defenses in place and aid an adversary in gaining access to a nuclear weapon. OC compiled the descriptions and justifications for 50X2-WMD classification concepts and reported these to the Interagency Security Classification Appeals Panel via ISOO in a letter dated January 5, 2012 (See Appendix K for a summary).

In assessing the purpose of topics, the working groups identified several instances where identical topics existed in multiple guides. This could lead to guidance inconsistencies in the future if not all versions of the same topic are updated when changes occur. To minimize the potential for this, a source topic was identified. The other versions were then rewritten to point to the source topic for classification guidance. As another portion of the topic assessment, the working group identified information not owned by DOE that was being classified by topics in DOE guidance. This occurred primarily because at the time of authoring the guidance the agency owning the information did not have a mechanism to distribute that guidance to DOE employees. For these topics, the guidance was removed, and the topics were rewritten to point to the guidance issued by the agency owning the information. These changes caused the number of topics referring (or pointing) to other DOE guidance or to guidance provided by other agencies to increase by 14 percent.

The deletions, declassifications, and other streamlining efforts caused enough reduction of topics in some subject areas to allow for the cancellation of some guides. Three guides and one bulletin have already been cancelled. Fifteen additional guides and eight bulletins have been recommended for cancellation.

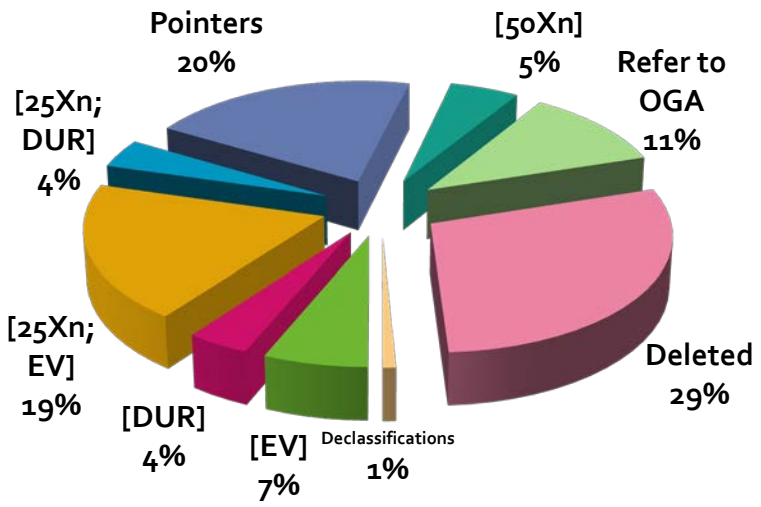


Figure 3. Recommended Guidance Conditions

VI. Summary

Within DOE, a comprehensive set of classification guides, which describe which information is classified and which is not, has been developed and maintained. DOE has historically relied on such classification guides as the basis for DC and DD classification and declassification decisions. This reliance on guides has ensured that consistent classification and declassification decisions are made throughout the DOE community and have reduced the likelihood of overclassification or an excessive duration of classification that would result in extra security costs and denying the public access to information that is not sensitive. For this process to function correctly, not only must a comprehensive set of classification guides exist, but these guides must be continually updated to identify information that no longer requires classification due to changes in circumstances. Therefore, it is imperative that a periodic review of classification guides, such as the one required in E.O. 13526, be conducted.

Since DOE has principal responsibility for the classification and declassification of RD and shares responsibilities with the DoD for the classification and declassification of FRD, the majority of the over 100 DOE HQ classification guides and bulletins contain RD and FRD topics that are not subject to the review required by section 1.9 of E.O. 13526. Out of those 100 classification guides and bulletins, over 2,800 NSI topics were identified for review in 78 classification guides and bulletins.

To conduct the E.O. 13526 review, OC relied on methods developed to ". . . maintain a continuous review of Restricted Data and of any Classification Guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data . . ." – a review

required by the Atomic Energy Act that is similar to the one now required by Executive Order for NSI. OC called together nearly 200 Federal and contractor employees who are subject matter experts to serve on 36 subject area working groups. The review, which took over 2 years, has resulted in recommendations that will streamline, clarify, and enhance DOE NSI classification guidance. Along with providing this report to ISOO, DOE will post this report on its website for examination by the public.

OC identified 77 keystones or key concepts that required classification. DOE developed clear justification for the classification of this information and identified appropriate classification levels and length of time that this information needs to remain classified. This review led to the recommended deletion of 30 percent of the topics from existing guidance and 22 declassifications. Further, the review resulted in a recommended 50 percent reduction in the use of event-based declassifications, removing ambiguity as to when the information will actually be declassified. Ownership of classified equities was clarified by recommending a 14 percent increase in topics pointing to other guidance for determinations.

With the addition of a new exemption from automatic declassification at 50 years in E.O. 13526, DOE will convert 7 percent of the NSI topic exemptions from 25X to 50X to ensure that information that would assist in the development, production, or use of WMDs is not made available to proliferators.

Once the recommendations are fully implemented, DOE will cancel 18 guides and 9 bulletins.

DOE plans to capture the results of this review with the software tools now used to create, maintain, and publish classification guides electronically. These tools will identify the basis for the classification of each DOE NSI topic, and as this basis changes, DOE will be able to immediately identify and update all affected topics. Revised guidance will be distributed in a timely manner for use by DCs and DDs to ensure the maximum release of information that is no longer sensitive. In addition, having each NSI topic and its basis now documented electronically will assist DOE to review the classification guidance (at least once every 5 years) to ensure that it continues to protect only that information that is critical to our Nation's security.

Through periodic on-site visits to HQ program offices and field elements that generate classified information, OC verifies that the classification guidance used by DCs and DDs is appropriate and current for the subject areas of information being classified or declassified. Also during these visits, a representative sample of classification decisions made by the DCs and DDs are examined to make certain that the proper guidance is used, the level and duration appropriately determined, and the associated markings correctly applied.

DOE fully recognizes that overclassifying information interferes with the public's right to know how its Government works while wasting limited resources to protect it. It also recognizes that underclassifying information compromises the national security that could result in a wide spectrum of damage to our country. Therefore, DOE strives to strike the proper balance through the issuance of classification guidance that reflects current world conditions. While limited resources and competing priorities may prevent us from attaining perfection in all cases, periodic

fundamental comprehensive reviews of our guidance will make an important contribution toward maintaining that delicate balance.

VII. Appendices

Appendix A. Electronic Publishing Tools

Over the past two decades, the DOE OC has made extensive use of electronic publishing tools to assist in guidance generation. Currently, DOE uses an extensible markup language (XML) editor (ArborText) to author and publish its classification guides in a PDF format. Version control (guide and checkout) is accomplished using SharePoint. Use of XML allows DOE to incorporate knowledge preservation information (metadata) into the electronic file. This metadata includes the following pieces of information:

- Keyword(s): A word or short phrase that describes the context/subject area of the topic. It comes from a predetermined list.

- Keystone(s): The classification concept(s) being protected by a topic. For example in the Safeguards and Security area, "Targeting Information" would be the keystone and the rationale would be because this would assist an adversary in the selection, targeting, or timing of an attack against a more vulnerable asset.

- Rationale: Reason why the associated guidance is classified or unclassified. (For example, for NSI topics the rationale metadata record would cite one or more appropriate classification categories from E.O. 13526 Section 1.4.)

- Genealogy: Shows how a particular topic in a guide has changed over time (i.e., chronology).

- Basis Link: The basis link indicates which other topic serves as the basis for the classification determination. The basis link is considered a unique topic developed from an original classification decision. The basis for a dependent topic may or may not exist in the same guide. The words "new topic" in this field identifies a new topic for the Original Classification Authority reviewing a guide for approval. Ultimately, with a proposed content management system, the guide authors will be able to assess the impact that a revision to a basis topic has on topics which are linked to it should the OCA determine that a classification level change or declassification should occur. For example, should a basis topic that classifies the xyz be declassified, it may require a change in all the dependent linked topics. The identification of basis links is crucial in guidance management in order to ensure promulgation of a change in classification in a timely and consistent manner.

- Usage: Information or examples of how particular guidance (topic) has been applied to make a classification determination ("case law").

- Background: A collection of hyperlinks or narrative text that provide supporting information to help understand a topic.

- Related Link: Lists other topics that cover information related to a given topic.

Once approved, the classification guides are placed into an eCGS that is available for use by DCs and DDs. The eCGS allows a full text search using PDF source files or metadata keyword list

searches using the XML source files. When viewing the guidance from the XML source file, the user can also view the information contained in the metadata fields described above.

This metadata will be updated once the FCGR recommendations have been approved. All the NSI topics will contain the keystone and rationale information. Where a keystone is identified by a specific topic, all other topics that classify information based on that keystone will identify the keystone topic as a basis link. Updating the metadata will link all the NSI topics in DOE classification guidance to specific information that has been identified as requiring classification. This will make it easier to generate accurate new topics that are applications of existing keystones and to uniformly change the classification of all existing topics when a keystone is no longer classified.

Appendix B. National Security Information Fundamental Classification Guidance Review charter dated November 4, 2010

Department of Energy
Washington, DC 20585

November 4, 2010

MEMORANDUM FOR ANDREW P. WESTON-DAWKES
DIRECTOR
OFFICE OF CLASSIFICATION
OFFICE OF HEALTH, SAFETY AND SECURITY

FROM: EDITH A. CHALK
DIRECTOR
OFFICE OF TECHNICAL GUIDANCE
OFFICE OF CLASSIFICATION

SUBJECT: National Security Information, Fundamental Classification Guidance Review Charter

In reply, please refer to HS92-10-N1-0079.

Attached for your review is the final draft of the National Security Information, Fundamental Classification Guidance Review charter. Please provide your approval by signing the signature page.

Attachment

cc: Donna Nichols, HS-92
Robert Cooke, HS-92
Glen Krc, HS-92
Johnnie Grant, HS-92
Thomas Callander, HS-92
Gregory Gannon, HS-92
Troy O'Baker, HS-92
Richard Lyons, HS-92
Joseph Stoner, HS-92
David Hix, HS-92
Nick Prospero, HS-91
Ken Stein, HS-93

Charter for the Department of Energy's
National Security Information Fundamental Classification Guidance Review

PURPOSE: The President of the United States has enacted into law Executive Order (E.O.) 13526, *Classified National Security Information*, dated December 29, 2009, which directs that a Fundamental Classification Guidance Review (FCGR) be conducted within two years of the effective date of the E.O., June 29, 2010. The Order states that Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current conditions and to identify classified information that no longer requires protection and can be declassified.

BACKGROUND: To comply with the requirements of the E.O., the Department of Energy (DOE), with the Office of Classification serving as facilitator, will conduct the National Security Information (NSI) FCGR. All DOE/National Nuclear Security Administration (NNSA) approved classification guidance, pursuant to the E.O., will be reviewed. The NSI FCGR will include an evaluation of such information to determine if the standards for classification (as stated in the E.O., Section 1.1) will continue to be met, taking into account a current assessment of likely damage that may occur following unauthorized disclosure of the information. As required in Section 1.9 of the E.O. and at the conclusion of the NSI FCGR, the Secretary of Energy will provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office (ISOO).

SCOPE: The NSI FCGR will be a systematic and comprehensive review of DOE's classification policy to identify NSI which continues to require protection, with the intent that all other information may be declassified and, where possible, made available to the public. All NSI within DOE's responsibility will be included. The review will encompass over 60 Headquarters (HQ) guides and 7 HQ Classification Bulletins. The NSI FCGR will also provide an evaluation of how NSI guidance topics are used by classifiers, and whether the intent of the guidance topics have been met as evidenced in derivative classification decisions.

PRODUCT: The NSI FCGR will be completed within the two year timeframe as required by the E.O., and will be accomplished by formation of multiple subject area review teams ("Working Groups"). The NSI FCGR will be conducted by knowledgeable personnel, including original classification authorities and agency subject matter experts, to bring a broad range of perspectives into the review. All Working Groups will report their progress and results to a Steering Committee, which will ensure consistency in approach and reporting. A basic project schedule is included in Appendix A.

Results that involve proposed NSI declassification actions will be submitted to the proper authorities via the Office of Classification for review and concurrence. Results will be compiled in a report to the Secretary that will detail the recommendations and supporting rationale. The report will be unclassified (with a classified annex) so that it may be made available to the public for informational purposes.

PROCESS:

Preparation of Classification Guidance Topics for Review – Office of Classification personnel will review all current guidance documents (guides, guidelines, bulletins) and extract the NSI topics. Topics will then be categorized, or "binned" in one or, where necessary, multiple subject areas. These subject areas will loosely align with E.O. 13526 classification categories (intelligence activities, foreign Government information, etc.) but may include more detailed division where practicable (e.g., Technical Surveillance Counter-measures (TSCM) as a subset of national security system capabilities). The total number of topics in a given subject area for all guidance documents will provide initial indications of the relative complexity of the subject area and review duration. For example, multiple teams may be required to review topics that address a variety of science and technology topics.

Steering Group Actions - The NSI FCGR will be initiated by the Steering Group, which will develop common review objectives to supplement the basic guidelines identified within the E.O., and will also ensure consistency of final product from each subject area Working Group. The Steering Group will consist of senior classification and program personnel from Headquarters and the field. The Steering Group will ensure development of a Working Group introductory briefing, which will include information on the background of the E.O., the guidance review process and Group communication structure. This briefing will be developed within the Office of Classification and will include informational items and learning objectives identified in Appendix B.

The Steering Group will identify a specific Subject Area (or partial Subject Area, such as Protective Force response) for formation of a pilot Working Group. The pilot Working Group will follow the basic procedure outlined by the Steering Group, with the knowledge that feedback from the pilot group will be used to adjust the guidance review process and communication structure to be provided to the remaining Working Groups.

Formation of Subject Area Working Groups - Each Working Group will have a chair and approximately six members who will be chosen for their subject area expertise in relevant technology and policy areas. Most members will represent DOE/NNSA programs and classification offices (field and HQ). One of the members of each Working Group will be a senior classification expert in the subject area. Where necessary, personnel from other agencies will be invited to participate in the Working Group. The Working Group member selection is critical to the success of the NSI FCGR effort. In addition, the progress of each working group will be monitored by a member of the Steering Group. Although participation as a Working Group member is voluntary, the member's home organization will be expected to strongly support each member's participation for that organization. It is expected that multiple Working Groups will be required for the areas of Science/Technology (X4), and safeguards & security systems (X8), and vulnerabilities (X8).

Operating Principles of Subject Area Working Groups - Based on the common review objectives and process structure/schedule provided by the Steering Group, each Working Group will conduct the review. Each Working Group is expected to review "difficult topics" (i.e., guidance topics that are suspected of inconsistent or incorrect application by classifiers), and to make recommendations for revised topic wording in the Working Group reports. Depending on the subject area complexity and size, interim status reports to the

Steering Group may be required. In general, a monthly status report is expected to be adequate. At any time during the review, additional direction may be sought from the Steering Group.

For DOE/NNSA owned information, each Working Group will identify the basic essential information that is being protected through classification, and why it should be protected under the E.O. The information being protected may range from details of some future activity, the vulnerabilities or capabilities of a security system protecting a nuclear weapon or Special Nuclear Material in storage, or information related to a foreign nuclear program that was provided in confidence to the U.S. Government.

The Working Group will then analyze the classification keystone protected by a topic, and then make a recommendation whether such information should retain current classification; cite a specific X exemption from automatic declassification at 25 years; or to propose a downgrade, upgrade, or declassification action for the information addressed by the guidance topic. The Working Group is to consider the following in its analysis:

- The balance between risking release of the information versus the cost of protecting the information. Assuming that the information meets the requirements of E.O. 13526, the cost of continuing to protect a piece of information may outweigh the benefit of protection. Even though a prior analysis may have concluded that the balance favored classification, this E.O. 13526 review will ensure consideration of acceptance a higher level of risk.

- If the information can be declassified, whether the information meets the criteria for protection as Sensitive Unclassified Information (e.g., Official Use Only or Unclassified Controlled Nuclear Information).

- Whether a topic, currently showing an exemption from automatic declassification at 25 years, may be more appropriately assigned a specific number of years for protection.

Supporting rationale to justify each recommendation must be provided. For information recommended to remain classified, a description of the damage to the national security must be considered, in the event of a future classification challenge. Each topic will be verified to have clear and understandable declassification instructions, and where based on a future event, such an event is reasonable, definite, and foreseeable. The Working Group will document their recommendations and supporting rationale in both periodic and final reports to the Steering Group. Should a Working Group member strongly disagree with a position taken by the team, that member may issue a minority report to the Steering Group.

Subject Area Working Group Logistics - For purposes of schedule development, it is assumed that the duration of an individual Working Group (formation, topic/keystone review, rationale development, recommendation reporting) may range from one month (in the case of a narrowly-scoped subject area encompassing a small number of topics) to six months (for complex subject areas or those that will require other agency coordination). It is also assumed that

service on a Working Group will be a collateral duty for the members. To ensure adequate coverage of all Working Groups by Steering Group personnel, it is likely that Working Group engagement will be staggered across a 15-month period (remainder of 2010 and all of 2011).

Review of Other Agency Equities – In the event that the NSI topics in a classification guide under review do not protect DOE/NNSA equities (i.e., DOE/NNSA agrees to identify, mark, and protect information that may appear in a DOE/NNSA document, at the request of another Executive Branch agency), then the Steering Group may choose to delegate the conduct of the review to the owning Agency. In this case, the Steering Group will send background review information (from the Subject Area Working Group introductory briefing), along with a requested completion date, to the owning Agency.

Compilation and Reporting to ISOO – On a quarterly basis, the Steering Group will report to the Director, Office of Classification, the progress and status of the Subject Area Working Groups. When a Working Group substantially completes its review and provides a draft recommendation summary, the Steering Group will note completion of the review and compile the results for discussion with ISOO. Progress briefings to ISOO, and when required, to the Interagency Security Classification Appeals Panel (ISCAP), may occur periodically. Early in 2012, a compiled report will be drafted to include the results of all Working Group reviews. A final report will be prepared for issuance by the Secretary prior to the two year deadline.

Classification Guidance Revision – As Working Groups complete their reviews and their recommendations have been accepted by Program Heads and the Director, Office of Classification, and where required, ISCAP, necessary revision to NSI topics contained in active classification guides will be the responsibility of the Office of Technical Guidance. In instances where significant revision is needed, Classification Bulletins may be issued in order to more rapidly promulgate the revisions to the derivative classifiers and derivative declassifiers.

Approved by:

Date: 11/24/10

Andrew P. Weston-Dawkes
Director
Office of Classification
Office of Health, Safety and Security

Attachments:

Appendix A - Proposed NSI Fundamental Classification Policy Review Schedule and Milestone Dates

Appendix B – Topical Areas for Development in the NSI FCPR Working Group Introductory Briefing Package

Appendix A - Proposed NSI FCGR Schedule and Milestone Dates

Task Identification	Target Date	Comments
1. Complete NSI topic binning process	5/28/10 Complete	Action complete; topic bins available on c-LAN portal.
2. Provide analysis of binning, suggest subject area divisions, suggest pilot Subject Area Working Group to Steering Group	7/8/10	
3. Obtain approval of FCPR Charter	HS-90 Approval	
4. Identify and finalize points-of-contact in program offices (for Steering Group and for Working Group assignments)	HS-90 Approval	
5. Identify Steering Group members	HS-90 Approval	
6. Form pilot Working Group; provide process and communication structure information to pilot group	Approval + 2 weeks	Pilot group active for 3 weeks – to report results back to Steering Group at +3 weeks
7. Review results with Steering Group and make adjustments to process and communication structure	Approval + 6 weeks	
8. Issue communication to program and field offices for Working Group assignments	Approval + 8 weeks	Request concurrence from supervisor for Working Group assignments at +2 weeks
9. Identify members and begin formation of Working Groups	Approval + 10 weeks	Include estimated working group timelines for start, intermediate reports, final report to Steering Group
10. Have all Working Groups finalized and begin analysis	Approval + 12 weeks	Final reports to Steering Group as Working Group completes recommendations and rationale
11. Quarterly status reports to Steering Group	1/1/11 and quarterly until 1/2012	ISOO updates and ISCAP approvals throughout, as necessary
12. Prepare final report to ISOO	2Q12	

Appendix B - Topical Areas for Development in the NSI FCPR Working Group Introductory Briefing Package

- E.O. 13526 Background Information, including classification categories and exemptions to automatic declassification, as described in Sections 1.4 and 3.3 of the E.O.
- Describe why the review is being conducted, what will happen to documents classified under new E.O., and what will happen to documents classified under prior EOs
- The NSI FCGR process workflow, including a basic timeline with intermediate milestones for each Working Group
- Review declassification instruction preference process described in the E.O. implementer –
  - date or event < 10 years from classification, coincident with lapse of sensitivity
  - date or event 10 years from classification, coincident with lapse of sensitivity
  - date or event not to exceed 25 years from classification
  - If information is thought to be exempt from automatic declassification, identification of the appropriate X code(s) – normally one, no more than two X codes should be cited
  - If none of the choices above are appropriate and intel/WMD is relevant, assignment of X code 50X1-HUM or 50X2-WMD
  - Use of classification duration extension (25 years from date of record if original date not reached; reclassify; both by original classifier)
- Summary of the current NSI-related topics contained in CG-HR-3, *Historical Records Declassification Guide*, which serves as the primary basis for topics in other classification guides that exempt DOE NSI from declassification at 25 years.
- Describe the review process to be used by the Working Group:
  - Determine whether or not the information is a DOE/NNSA equity, and is then classifiable by DOE derivative classifiers
  - Discussion by the Working Group to identify or describe damage to national security that would be caused by release of the protected information - will HS-90 be able to defend position in case of a challenge?
  - What is the basic fact that the topic is protecting? Is it merely a pointer back to the same topic in a different guide?
  - Is each topic correctly and clearly written?
  - Is the topic adequate? Are there known issues with use of the topic by DCs?
  - Are the declassification instructions clearly written and achievable?
- Provide examples of good and bad declassification instructions
- How to define the need for an X code (need a narrowly defined area of information; specifics associated with something non-obvious can be identified and placed in metadata when the guide is revised; does the information really require classification more then 25 years in the future?)
- Provide a reporting format for Working Group team report-back to the Steering Group, both for status reports and proposed changes; requests for clarification, and reporting of areas of disagreement
- Discussion on assignment of multiple X codes
- Process to be followed if another "75 year" case is identified
- Identification of which current topics, by guide, the working group is expected to review

Appendix C. Thirty-six subject areas

Thirty-six Subject Areas

1 – Physical Security Systems and Vulnerabilities

2 – Special Access Programs

3 – Technical Security Countermeasures

4 – Critical Infrastructure Information

5 – Transportation Safeguards System

6 – Cyber Security

7 – Information Security

8 – TEMPEST, COMSEC, and Cryptology

9 – Material Control and Accountability

10 – Graded Security Protection

11 – Intelligence and Counterintelligence

12 – Enrichment

13 – Environmental Sampling

14 – Material Protection Control and Accountability

15 – Nuclear Smuggling

16 – Nuclear Materials

17 – Materials Disposition

18 – Power Systems

19 – Russian Materials

20 – International Safeguards

21 - Radiological Dispersal Devices

22 – Weapon Outputs

23 - Malevolent Dispersal/Threat Messages

24 - Radiological Emergency Response

25 - Weapon Production and Military Use

26 – Improvised Nuclear Devices

27 – Cancelled

28 – Weapons Two

29 – Testing

30 – Civilian Radioactive Waste

31 – Weapons One

32 – Radiation Hardened Microelectronics

33 – Treaties

34 – Chemical/Biological Programs

35 – NA-20

36 – High Power Radio Frequency

37 – United Kingdom

Appendix D. DOE steering committee members

Steering Committee

Edith Chalk, Department of Energy, Director, Office of Technical Guidance, Chairman

Donna Nichols, Excalibur, Executive Secretariat

Tom Anderson, Department of Energy, Office of Environmental Management, Member

Don Barnes, Department of Energy, Office of Nuclear Energy, Member

Walter Dykas, Department of Energy, Office of Science, Member

Reece Edmonds, National Nuclear Security Administration, Security Operations Division, Member

Robert Lange, Department of Energy, Office of Nuclear Energy, Member

Ty Sanders, Department of Energy, Office of Environmental Management, Member

Appendix E. DOE action/outcome chart

FCGR required actions and expected outcomes for Working Groups (listed in recommended order)

For each topic currently classified:

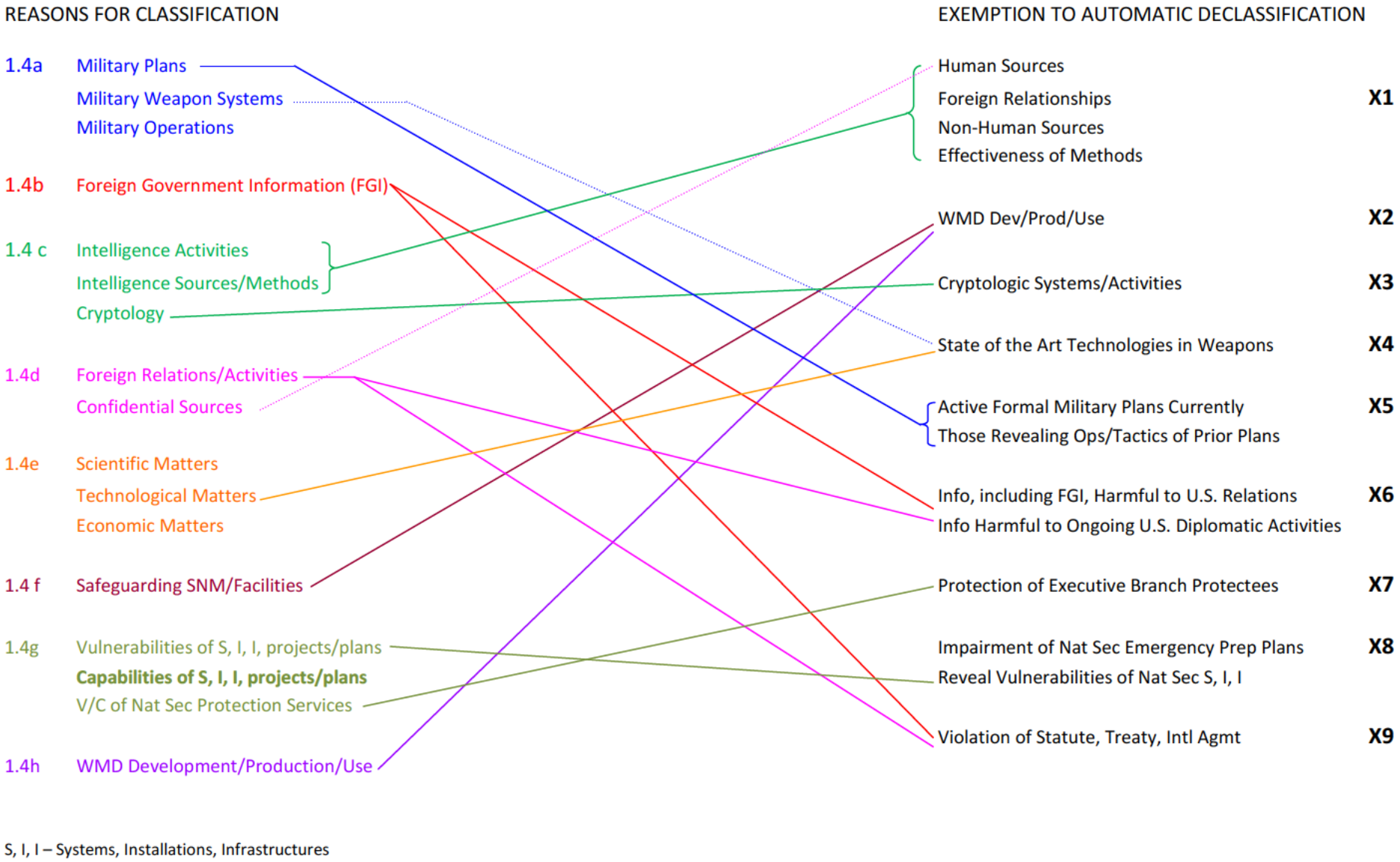
Action:	**Outcome:**
1- Determine the current basis for the topic, where possible. For example, most DOE facility security related topics actually are based on a few topics in SS-4. Likewise, material transport topics (e.g., schedules, routes, vehicle design details) are based on a few topics in TSS-3. If a clear basis topic is identified for a "dependent" topic, ensure that the relationship is documented. Also, assess what "key concept" is being protected by the topic; what is it that we are ultimately protecting?	Information developed from this step will be added as the "basis link" and "keystone" in the metadata for that topic when guidance is revised. NOTE: Where a dependent topic is identified, in most cases the classification level and duration will agree with the basis topic; however, some cases may be different. Be sure to analyze and document justification where your dependent topic may be different.
2 - Assess whether the information is owned by, produced by or for, or is under the control of the USG [E.O. 13526, Section 1.1 (2)]. Furthermore, is the information owned by DOE, or possibly another USG agency?	This information will allow you to determine that the information is, indeed, owned by the USG, and to identify the "owning agency" of the information equity. If an agency is other than DOE, and the guide is not a joint guide (i.e., signed by DOE and the other agency), mark for referral to that agency. If a joint guide equity, or solely a DOE equity, continue analysis process.
3 - Determine the E.O. Classification Categories [Section 1.4(a) – (h)] by which the information is classified.	If the information protected by the topic does not fall into (a) – (h), then it cannot be classified as National Security Information.
4 – Identify/describe the damage to national security that would result from the unauthorized disclosure of the information protected by this topic.	Provides the basis for identifying the classification level or (range of levels) for the topic. If a range, then identify the qualitative differences between level.
5 – Based on the answer to 4, does the cost of continuing to protect the information outweigh the benefit of protection?	If the answer is that cost of protection outweighs the benefits, then assess whether a lower classification level, or declassification would be appropriate. In this regard, make a determination, with supporting justification, as to whether the classification of the topic should be upgraded, downgraded, or declassified.
6 – Identify when the information no longer requires protection. This criterion should be a specific event that can be described; the event should be clearly determinable (reasonably definite and foreseeable). If an event cannot be described, then determine a date (or duration ≤ 25 years), past which the information would no longer require protection. If classification duration is greater than 25 years, then identify the appropriate exemption code from E.O. Section 3.3(b).	This step allows analysis of existing declassification dates/events. If a 25X duration is identified, then a corresponding topic MUST be included in CG-HR-3. In the extraordinary case where a 50 year duration is not considered sufficient, and only in cases for *protection of the identity of a confidential human source or a human intelligence source*, or *key design concepts of Weapons of Mass Destruction,* then a specific request must be made to the Interagency Security Classification Appeals Panel (ISCAP) via the Director, Office of Classification.

7 – As determined by step 6, provide accurate declassification instructions (an event or a "year-duration" with no exemption is preferred). Other declassification instruction issues to look for include: a) an EV should not be shown if the topic must be referred to another agency; and b) note that some declassification instructions may impact protection of the same information within other government agencies, so consider inclusion of a CAUTION with the topic.	This will provide consistently and accurate higher quality declassification instructions.
8 - Be sure to assess any known issues (difficulty in application, inconsistent use, etc) with the topic.	Such a qualitative review is required by E. O. Section 1.9.
9 – Address the following miscellaneous guidance "housekeeping" issues: a. Delete any classifications shown for parent topics b. Remove guidance statements from NOTES and place in topics. c. If a range of categories and/or levels are included, such as "CRD/CFRD maybe NSI," ensure there are clear instructions as to when each category is relevant and how the range of classification is applied. d. If a topic "points" to multiple possible sources of information (e.g., Classify based on information revealed"), add an explanation at the beginning of the guide or chapter, so that the reviewer will be better able to discern next steps (identify agencies/programs, etc.). e. If dealing with FGI topics, assess need for including a TFNI marking.	Continued assessment of the quality of guidance topics.

Appendix F. DOE steering committee schedule

Steering Committee Meetings										
4/28/2011	6/30/2011	8/11/2011	9/8/2011	10/5/2011	11/3/2011	12/1/2011	1/12/2012	2/9/2012	3/15/2012	4/x/2012
SAP (WG 2)	**WPMU** (WG 25)	**UK topics** (partials of WGs 12, 16, 24, 28, 29, 31, 37)	**Vulnerabilities** (WG 1) - Callander	**Russian** (WG 19)	**Power Systems** (WG 18)	**Environmental** (WG 13)	**Enrichment** (WG 12)	**Smuggling** (WG 15)	**InfoSec** (WG 7)	reserved for review of draft FCGR report
TSCM (WG 3)	**CII** (WG 4)	**TC&C** (WG 8)	**IND** (WG 26)	**TSS** (WG 5)	**HPRF** (WG 36)	**Int'l Safeguards** (WG 20)	**NA-20** (WG 34)	**Cyber** (WG 6)		
Microelectronics (WG 32)	**Weapons 1** (WG 31)	**Materials Disposition** (WG 17)	**Weapons Outputs** (WG 22)	**Material Protection** (WG 14)	**Materials** (WG 16)	**Weapons 2** (WG 28)	**IN/CI** (WG 11)	**GSP** (WG 10) - Callander		
	RDD (WG 21)	**ChemBio** (WG 34)	**SLD** (WG 27)	**Disp/Threat** (WG 23)	**Testing** (WG 29)	**HR-3** (WG 38)		**MC&A** (WG 9) - Callander		
			CIV RadWaste (WG 30)		**Treaty** (WG 33)					
					Nuc Emergency (WG 24)					

Appendix G. DOE reasons for classification chart



S, I, I – Systems, Installations, Infrastructures

Appendix H. DOE steering committee reporting chart

2011 NSI FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
TOPIC ANALYSIS

Date:			
Working Group Name:		**Working Group #:**	
Leader:			
Members:	*list members of the WG effort, even if a "formal" WG was not constituted.*		

Summary of information reviewed by Working Group:	*Provide a general description of what the NSI topics in this area cover; e.g., protection of transportation-related information for movement of SNM, protection of information concerning vulnerabilities of a physical protection system; USG negotiation positions. If the WG covers topics from multiple guides, provide a brief summary of each.*

INITIAL ACTION OFFICER REVIEW

Total Number of Topics Identified for Preliminary Review:	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Pointing to Other Guidance (application of topic dependent on specific situation):	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Driven by Other Basis Topic (topics in other guides, or other topics from same guide):	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Referred to Another Agency (topics concerning information for which DOE has no equity):	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Requiring WG Analysis (topics not covered above, for which DOE has sole or shared equity):	*If WG includes multiple guides, topical counts should be listed separately*

2011 NSI FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW
WORKING GROUP RESULTS

Working Group Name:	**Completion Date:**

WORKING GROUP REVIEW:

Number of Topics Retained/Rewritten:	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Added for Clarity:	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Deleted:	*If WG includes multiple guides, topical counts should be listed separately*
Number of Topics Referred to Another Agency (joint equities):	*If WG includes multiple guides, topical counts should be listed separately*

REVIEW SUMMARY:

Specific keystones identified:	*List each keystone identified by the WG. Attach additional pages if needed.*
Changes in Classification Level/Category Recommended:	*List each declassification or downgrade, with corresponding justification. Attach additional pages if needed.*
Summary of changes in declassification instructions:	*Include such changes as reduced occurrence of 25X topics, shoretned duration, clasified declassification event, etc.) Include number of topics affected. Attach additional pages if needed.*
Summary of major improvements:	*Provide a short narrative to major improvements to each guide. Attach additional pages if needed.*

2011 NSI FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW

STEERING COMMITTEE COMMENTS

Appendix I. Thirty-six working group reports

Working Group 1– Physical Security Systems and Vulnerabilities

Current Policy

The current guidance for physical security systems and associated vulnerabilities encompasses information related to the physical security systems, including sensors, barriers, and the guard protective force (PF), for Department of Energy (DOE) sites and facilities, protecting nuclear weapons, Special Nuclear Material (SNM), classified information, and other assets.

Background

The current guidance is contained in *Classification and UNCI Guide for Safeguards and Security Information* (CG-SS-4), *Evaluation of Commercial Technologies for Use as Security Subsystems* (TNP-22), *Guidance for Security Protective Force Command and Control Systems* (TNP-26), and *Classification Guidance for Classified Meeting Locations at DOE/NNSA or DOE/NNSA Contractor Sites or Facilities* (TNP-32).

The current National Security Information (NSI) safeguards and security topics for physical security systems, operations and associated vulnerabilities (one hundred and seventy-eight in total) consist of the following:

- Twenty topics exempt from automatic declassification at 25 years because the disclosure of such information would reveal information that would assist in the development, production, or use of weapons of mass destruction (WMD) (25X2).
- One hundred and thirty-three topics exempt from automatic declassification at 25 years because the disclosure of such information would reveal current vulnerabilities of systems, installations, or infrastructures relating to national security (25X8).
- One topic exempt from automatic declassification at 25 years under all 9 exemption categories listed in Executive Order (E.O.) 13526 1.4 (25X1,2,3,4,5,6,7,8,9).
- Eight topics that are declassified at 25 years.
- Nine topics with an event-driven declassification.
- Seven topics that are based on other topics.

Analysis

The following six keystones were identified:

- Exploitable Design Information - Adversary exploitation would lower expected performance of a DOE developed or modified element/component.
- Assessed Performance - Performance values calculated, used, or determined in Vulnerability Assessment (VA) analysis that would assist adversary attack optimization.
- Deficient Performance - Performance values calculated or determined in VA analysis that would assist adversary attack optimization by exploitation of the weakness or deficiency.
- Planned Response - Assists adversary attack optimization.
- Targeting Information - Assists adversary identifying or locating a vulnerable asset, or timing an attack when an asset is vulnerable.

- Novel Method/Technique - DOE developed method/technique that defeats or degrades performance/functioning of a security element/component.

E.O. 13526 1.4 (f), (g), and (h) apply to all topics associated with the protection of SNM. Acquisition of SNM is perhaps the most important step in constructing a nuclear weapon or Improvised Nuclear Device (IND) (i.e., a WMD). For all topics associated with the protection of classified information, 1.4 (g) and (h) apply. Much of DOE classified information is Restricted Data (i.e., weapon design, nuclear material production methods). This information is extremely valuable to WMD proliferators; thus for all NSI information exempted from 25-year declassification, 25X2 applies.

Many classified topics in CG-SS-4 are based on a small set of topics that, while not identified as such, function as classified keystones. For example, dozens of topics for physical security components base classification on a vulnerability table or method/technique topics. Elimination of many of these "pointer" topics improves guide clarity and usability.

Recommendations

A recommendation below to no longer classify information does not mean the information will not be protected. Much of this information will continue to be controlled using either Official Use Only (exemption #7, Law Enforcement information) or Unclassified Controlled Nuclear Information. Many of the proposed changes below are based on the principle that information can be classified only if all available indicators are protected commensurately.

Revise the guidance to reflect the classification of the keystones as identified. Suggested revisions are summarized below:

- Only exempt, from automatic declassification at 50 years (50X2-WMD), information about a specified physical security component/element. For a security component expected to be used for more than 50 years, guidance for that specific component will be developed and approved with a 50X2-WMD exemption.
- Downgrade maximum NSI classification of information relating to physical security systems and their vulnerabilities to Secret (S), because it is neither practical nor reasonable to expect DCs to make these judgments. Exceptions requiring TS to be handled by a designated TS original classifier authorized to make them for site or program safeguards and security information.
- Cancel guidance for non-OST inter-site shipments of Category I/II SNM. Specific shipment guidance should instead be developed and approved when needed based on OCA decisions. Shipment information (planned route, shipment times, etc.) concerning one or a series of them should be protected pending development of specific guidance tailored to the particular circumstances of that shipment (or series of shipments).
- Replace vulnerability with Protection Effectiveness (P_E) determinations (quantitative analyses validated through performance-based testing) for more objective derivative classifications.
- Replace a vulnerability determination for Category II or lesser quantities of SNM, classified information/matter, and other Government property, with a determination by the Officially Designated Federal Security Authority (ODFSA) or Officially Designated

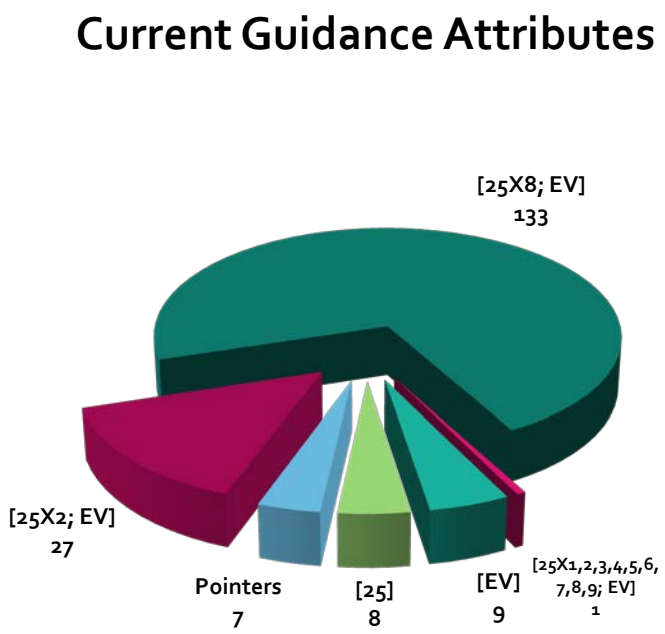
Security Authority (ODSA) (the official security authority at a site/facility responsible for the protection of an asset) that protection is unacceptable (meaning that exploitation by an adversary could result in damage to national security such as theft of SNM) under the Deficient Performance keystone. Declassify when the ODFSA or ODSA determines protection is acceptable, and do not exempt from automatic declassification at 25 years.

- Classify under the Deficient Performance keystone, the fact of credible roll-up to Category I, II, or III SNM quantity for a location only authorized to contain a lower category of SNM, and to declassify when corrected.
- Classify DOE developed/modified security alarm management and control system designs or operational characteristics that can be exploited by an adversary to lower its expected performance, to exempt this under 25X2, and declassify when the security alarm management and control system is no longer used under the Exploitable Design Information keystone.
- Limit classification of duress alarms, concealed sensors, and DOE developed/modified sensors to design or operational characteristics whose exploitation would lower expected performance under the Exploitable Design Information keystone, and to change the declassification from when the sensor is no longer related to an installed sensor or one considered for installation to when exploitation would no longer lower expected performance at any DOE site/facility.
- Set a single classification level for DOE developed or modified active or passive delay/deterrent/denial system design, location, details of construction, or operational characteristics that can be exploited by an adversary to lower the expected performance of the active delay/deterrent/denial system under the Exploitable Design Information keystone.
- Classify the qualitative and quantitative assessment of the consequences of adversary exploitation of a deficiency and related assessed performance values, and exempt the quantitative values under 25X2 for any element/component still in use.
- Delete redundant guidance for intrusion alarm reporting/assessment, passive/active delay function, tamper alarm function, and tactical communications, as this is already addressed by method/technique guidance.
- Classify "novel" methods/techniques.
- Replace an overall system analysis for a method/technique with an individual element/component level analysis, and delete necessary/sufficient classification level determinations. Set a single classification level for a specific element type (e.g., method to degrade intrusion detection sensors).
- Classify combinations or codes providing direct access to Category I or II SNM under the Exploitable Design Information keystone.

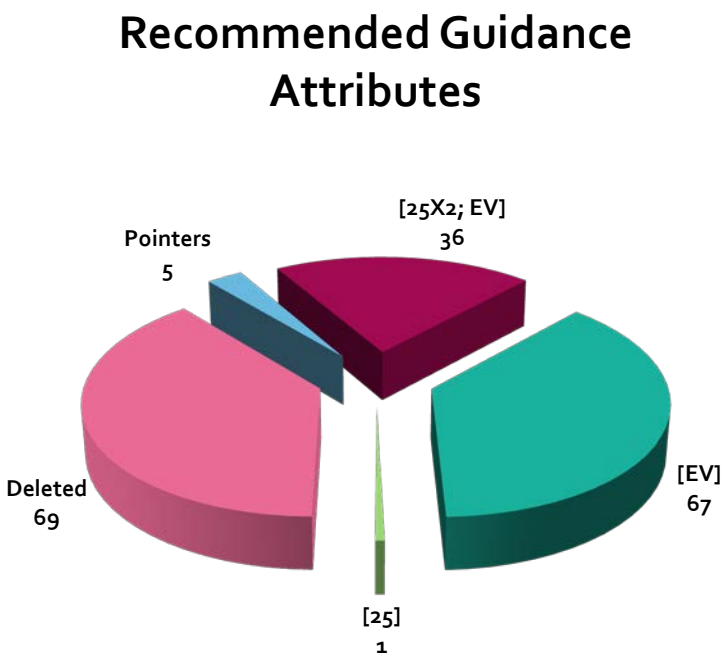
If implemented, this would result in the following changes:

- Sixty-nine topics deleted.
- No topics exempt under 25X8.
- Thirty-six topics exempt under 25X2.
- One topic that is declassified at 25 years.
- Sixty-seven topics with an event driven declassification.
- Five topics that are based on other topics.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 2 - Special Access Programs

Current Policy

Executive Order 13526 authorizes the Secretary or Deputy Secretary of Energy to create unique security cells called "special access programs" (SAPs) within the Department, but only upon the specific finding that: "(1) a vulnerability of, or threat to, specific information is exceptional; and (2) normal criteria for determining eligibility for access to information classified at the SAP are not deemed sufficient to protect the information from unauthorized disclosure; or (3) the program is required by statute." Many routine operational and security functions that would otherwise be unclassified usually are classified when structured for a SAP.

Background

The guidance was located in the first chapter of the *Annex to Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4A). The 50 topics in this guide identified the aspects of a special access program that required protection through classification. These topics classified information because of the enhanced security controls in place as part of the special access program. This information was to be declassified when the programs were declassified. Much of the information regarding U.S. Government programs for safeguarding nuclear materials or facilities and national security related scientific, technical, or economic matters normally is classified NSI. When information is determined to be of such extreme sensitivity that normal controls are deemed insufficient to provide adequate protections, a SAP may be established to provide the requisite protection.

Analysis

All of the National Security Information (NSI) topics in this guide are consistent with sections 1.4(e) and 1.4(f) of E.O. 13526.

The following keystone was identified: information classified because of the enhanced security controls in place (i.e., the information is in a SAP).

The existing guidance is not always clear as to why a topic is classified. In additon, the declassification events for the information do not match the reason that the inforrmation is classified.

It is DOE policy to classify safeguards and security information that could (1) provide meaningful assistance to a malefactor in the theft of Special Nuclear Material (SNM), sabotage of DOE facilties or assets, or composing a credible nuclear threat message; (2) be exploited by a malefactor or by a foreign intelligence service to either enhance its intelligence collection efforts or thwart U.S. counterintellignece efforts; or (3) provide assistance in gaining unauthorized access to classified information, including that in secure communications or in Information System (IS) equipment. This continues to be the cornerstone of the DOE safeguards and security classification policy.

Information related to a SAP is classified when that information is determined to be a part of the security controls for the SAP. Once these controls are removed from the information, classification is no longer required unless the information itself is classified. At the same time, the existence of a special access program may be declassified while the information handled by the SAP remains classified. For these reasons, the declassification events for SAP information should either be "when the enhanced protection measures have been removed" or "when the enhanced protection measures have been removed and the information is not classified by other DOE classificaiton guidance" depending on whether the information in and of itself is classified.

Recommendations

Better defining why the information requires protection allows for the reduction of the total number of topics in the guide. The total number of topics requiring classification of the corresponding information was reduced from 50 to 36. Additional changes include a more appropriate and easily determinable declassification event and an update to the wording for consistency.

Working Group 3 - Technical Security Countermeasures

Current Policy

The current guidance for the Technical Security Countermeasures (TSCM) program contains several inconsistencies that lead to the over-classification of information. The structure and phrasing of some of the topics causes confusion as to which of many topics is applicable to a particular piece of information. This leads to the application of a topic to a piece of information with an incorrect classification level and an incorrect duration of classification.

Background

The guidance is located in the second chapter of the Annex to Classification and UCNI Guide for Safeguards and Security Information (CG-SS-4A).

The chapter contains 27 National Security Information (NSI) topics, 24 of which meet the requirements for classification. Eighteen of these topics are exempt from automatic declassification. The declassification instructions for these topics are:

- Eight topics have an event driven declassification.
- Five topics require declassification at 50 years.
- Four topics require declassification at 25 years.
- One topic requires declassification at 10 years.
- The remaining six topics are not exempt from automatic declassification as identified above, but are declassified at 10 years.
- Three remaining topics point to other guidance.

Analysis

Three keystones require protection:

- Date of service.
- Capabilities/limitations of the TSCM program.
- Identification of a vulnerability/hazard.

The date of service requires a classification duration of 25 years. This decision was based on how long this information would be useful to an adversary in determining whether a planted device has been detected and in determining whether any information collected by the device could be trusted as accurate.

The capabilities/limitations of the TSCM program were determined to be exempt from automatic declassification at 25 years. The capabilities of the TSCM program slowly change with the introduction and replacement of techniques and equipment. However, the replacement of single (or a few) techniques or pieces of equipment does not alter the capabilities of the program drastically enough to prevent disclosure of the now former capabilities from revealing the current capabilities. Because of this, it is not possible for a derivative classifier to determine how many

techniques or pieces of equipment need to change before the linkage between former and current capabilities is broken. Comparing former capabilities to current capabilities indicate that 25 years is insufficient time for any linkages to break. By 50 years, however, the underlying technology has changed significantly enough that current capabilities would not be revealed. The identification of a vulnerability/hazard was determined to no longer be sensitive once the vulnerability/hazard is corrected.

Recommendations

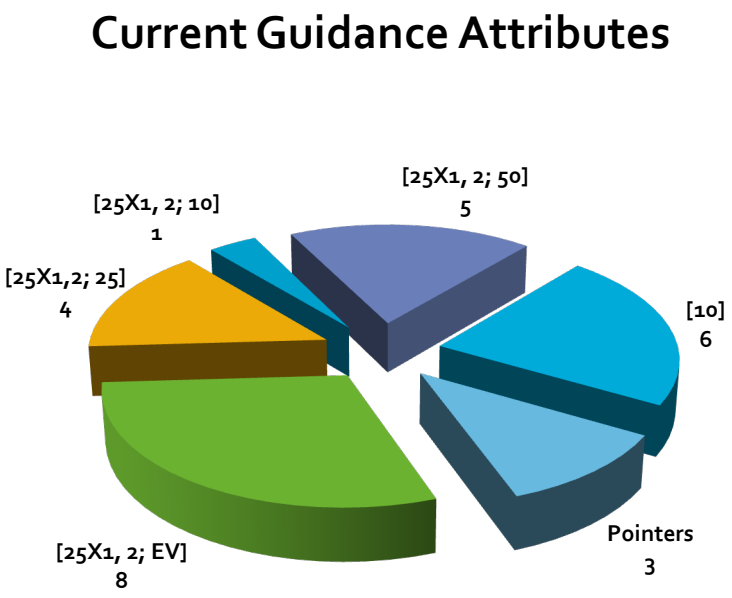
The guidance topics were rewritten to reflect the classification of the keystones. This resulted in the following changes to guidance:

- The number of event driven declassifications reduced from 8 to 4.
- All 18 exemptions from automatic declassification became date driven rather than event driven.
- Nine topics were eliminated because of redundancy.
- Ten topics were added to aid the identification of mechanisms that would reveal the capabilities/limitations of the TSCM program (keystone 2).
- Ten topics that address keystones 1 and 2 were divided into 24 topics that more discretely identify the classified information requiring protection, which will result in the classification of less information.

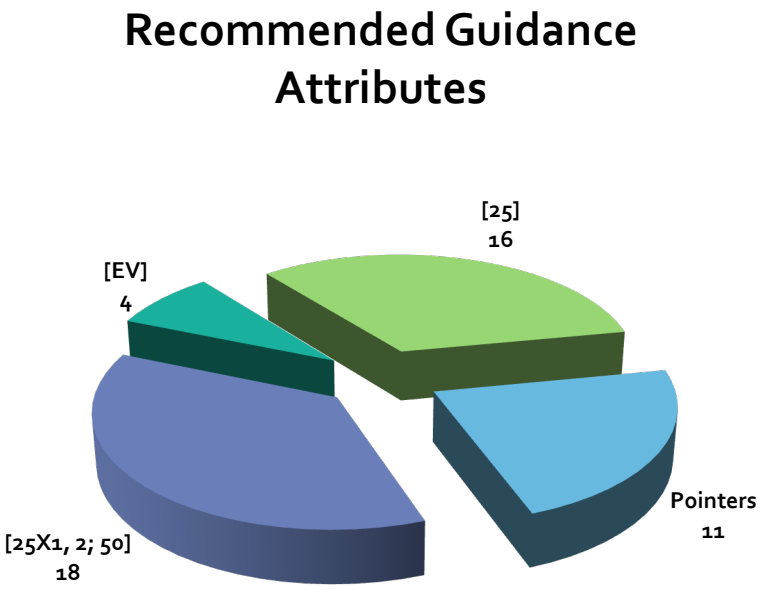
These changes resulted in new guidance that contains 49 NSI topics. The topics consist of the following:

- Eighteen topics that are declassified at 50 years.
- Sixteen topics that are declassified at 25 years.
- Four topics with an event driven declassification.
- Eleven topics that point to other guidance.

The following chart identifies the declassification instructions used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 4 - Critical Infrastructure Information

Current Policy

Homeland Security Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection* identifies the Department of Energy (DOE) as the sector lead for energy, including the production refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities). In this role, the Department performs vulnerability analyses of these facilities and makes recommendations on how to improve their security. The Department also has ownership of the Strategic Petroleum Reserve (SPR) and the Power Marketing Administrations (PMAs). The current guidance for Critical Infrastructure Information (CII) addresses the protection of information related to the operations of the Bonneville Power Administration (BPA) (one of the PMAs), the operations of SPR, and security assessments of foreign and domestic non-nuclear energy sites.

Background

Classification guidance in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4) addresses the performance of the vulnerability assessments of commercial facilities. Classification guides also exist to address classification concerns at the SPR and BPA, one of the PMAs. The SPR and BPA guides interpret the broader CG-SS-4 topics in order to apply appropriate classification levels based on the damage to national security that unauthorized disclosure of the information would have for SPR and BPA. Two classification bulletins, *Guidance for International Energy System Reliability Analyses* (TNP-31) and *Guidance for Reliability, Survivability, Resiliency Analyses* (TNP-35), address activities conducted by DOE's Office of Infrastructure Security & Energy Restoration (ISER) (OE-30). These bulletins also interpret the guidance from CG-SS-4 for proper application for the ISER programs.

These topics consist of:

- Fifty-four topics exempt from declassification at 25 years.
- Sixteen topics with an event driven declassification.
- One topic that is declassified at 25 years.

Because the CG-SS-4 topics serve as the bases for the classification of DOE CII, these topics were examined to determine what CII should be classified by DOE.

Analysis

No keystones were identified for the information.

The application of CG-SS-4 CII topics requires a subjective determination by a derivative classifier that the information impacts national security. In practice, this necessitates a judgment reserved for an original classification authority. Organizations that work with CII, such as OE-

30, should make use of original classification authority, when necessary, to make original classification determinations for CII.

A classification determination requires that the unauthorized disclosure of CII cause describable damage to national security. Most DOE efforts in this area involve coordination with and assisting the commercial sector, or government organizations with strong links to the commercial sector (e.g., BPA), to improve the security and reliability of their networks and systems. While there are many possible scenarios with consequences that may arguably damage national security, in most cases classification only encumbers DOE communications with the commercial/private entities and delays or prevents the implementation of corrective or compensatory measures for identified vulnerabilities. DOE work to date has not identified any energy sector vulnerabilities or scenarios that clearly and demonstrably damage national security. In addition, safety information that must be made available to state and local governments as a part of safety and other regulatory requirements cannot be classified.

Recommendations

DOE does not currently have the need to derivatively classify any energy-related CII. This determination does not prevent DOE from exercising original classification authority on a specific item of CII in the future, if it can be clearly demonstrated that damage to national security would occur if the information were disclosed. It also does not preclude another agency, such as the Department of Homeland Security or the Department of Defense, from classifying CII. This determination will affect the topics in CG-SS-4, CG-BPA-1, CG-SPR-4, TNP-31, and TNP-35.

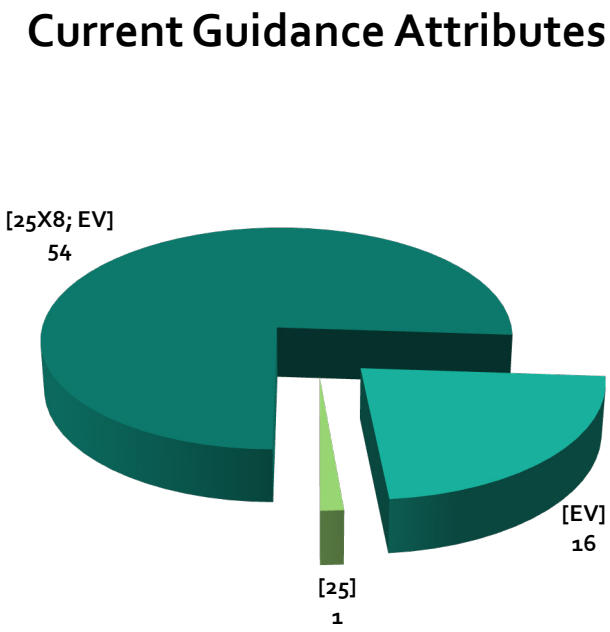
Therefore, it is recommended to:

- Remove derivative classification determinations for CII from DOE classification guidance.
- Add clarifying language to DOE classification guidance clearly stating that original classification determinations will be made for new CII where there is a potential that disclosure of the information will cause definable damage to national security, such as a defined monetary loss, a defined loss of life, a defined loss of property, or a defined cost of recovery.

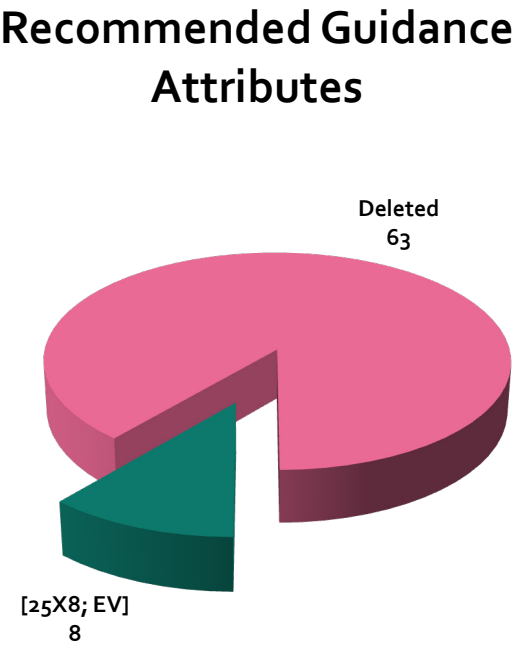
These recommendations would result in the following changes:

- Sixty-three topics would be deleted.
- Eight topics would be rewritten to remove reference to CII.

The following chart identifies the declassification instructions used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 5 - Transportation Safeguards System

Current Policy

The Transportation Security System (TSS) is operated and managed by the Office of Secure Transportation (OST), which is under the direction of the National Nuclear Security Administration (NNSA). The mission of the OST is the safe and secure transportation of government-owned Special Nuclear Material (SNM) nationwide in support of the DOE/NNSA nuclear research and production programs.

Classification guidance for the TSS encompasses information related to the shipment and receipt of nuclear materials, the operations of the OST, the design and operation of the Safe Secure Trailer (SST) and support vehicles, and the design and operation of the Secure Railcar (SR) and support vehicles.

Background

The current guidance is contained in the *Transportation Safeguards System Classification and Unclassified Controlled Nuclear Information Guide* (CG-TSS-3). The guide contains 152 National Security Information (NSI) topics. Of these, 124 topics state an exemption from automatic declassification at 25 years.

Of the remaining topics that are not exempt from automatic declassification as identified above:

- Ten topics have an event driven declassification.
- One topic that is declassified at 25 years.
- Three topics that are declassified at 10 years.

The remaining 14 topics point to other guidance.

After removing the topics pointing to other guidance, the remaining 138 topics were examined.

Analysis

Three keystones that required protection are:

- Targeting information that would be useful in planning an attack by identification of a shipment contents or the timing and location of a shipment.
- Design information that if exploited by an adversary would result in lowering the expected performance of the component.
- Information that would assist an adversary in planning or executing a successful attack by lowering the performance of a security system or component.

Six topics incorrectly exempted information from automatic declassification at 25 years because the release of the information would impair the effectiveness of an intelligence method currently in use, available for use, or under development. This was determined to be an erroneous

application of this exemption, as the information was classified to reduce the potential for an attack against the TSS, not to protect the identification of an intelligence method.

One topic incorrectly exempted information from automatic declassification at 25 years because the release of the information would reveal the identity of a confidential human source. This too was an erroneous application of this exemption, as the information was classified to reduce the potential for an attack against the TSS, not to protect the identification of an intelligence source. Two topics incorrectly exempted information from automatic declassification at 25 years because the release of the information would reveal information that would impair U.S. cryptologic systems or activities. The information should have been exempted to prevent an adversary from gaining access to a nuclear weapon.

Thirteen topics exempted information from automatic declassification at 25 years because the release of the information would reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security. While the TSS can be considered a system, installation, or infrastructure relating to the national security, information related to capabilities and vulnerabilities of the TSS are more appropriately exempt from automatic declassification because the release of the information would reveal information that would assist in the development, production, or use of a weapon of mass destruction (WMD). This is because the TSS transports nuclear weapons and access to this information would assist in acquiring these weapons.

It was determined that targeting information required protection before and while a shipment was occurring. Because a trip may include shipments to multiple sites, and OST does not classify the routes available for use, the duration of classification for this information needs to extend until the trip has completed. If the receiver of a shipment declassified the targeting information after shipment arrival, an attacker could determine the route being used for the remaining shipments in a trip and plan an attack accordingly. Because the receiver does not need to know, cannot determine when the trip will be completed, a 30-day duration following departure of OST from a site was chosen for this information to allow for completion of the all trip segments prior to declassification of the targeting information.

Exploitable design information for a component requires protection until the component is no longer used in an active transport system. Access to this design information would allow an adversary to develop and test methods that would lower the expected performance of these components and therefore increase the likelihood of a successful attack. Because the current systems in use are evolutions of systems originally fielded in the early 1970s, a duration of 50 years does not provide sufficient protection for the information. Because access to this design information would impair the effectiveness of the defenses in place and would aid an adversary in gaining access to a nuclear weapon, this information meets the criteria of E.O. 13526, Section 3.3(h)(1)(B) to be exempt from declassification at 50 years. Justification for these topics was sent to the Interagency Security Classification Appeals Panel (ISCAP), via the Information Security Oversight Office (ISOO), for approval.

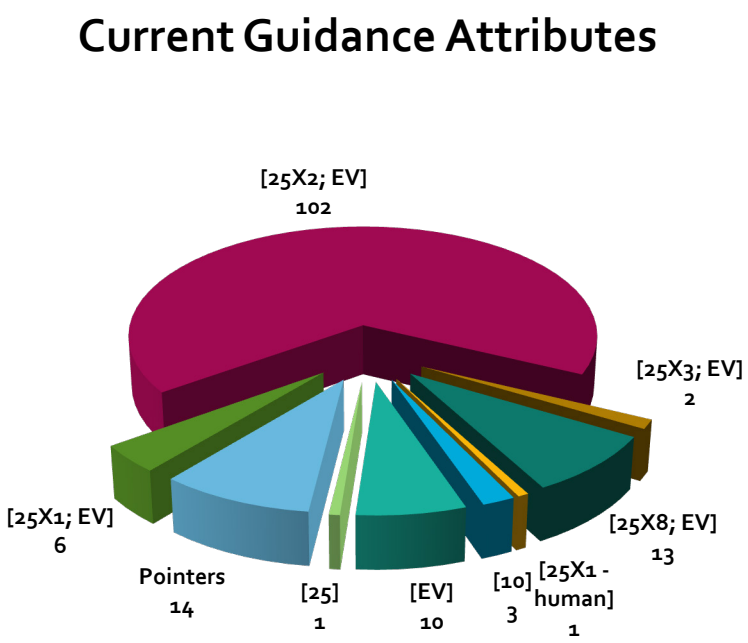
Separate from design information, other information about tactics and defense strategies used by OST requires protection through classification. Exploitation of this information by an adversary in the planning or execution of an attack would result in a higher likelihood of a successful attack. Because this type of information changes over time, it does not require the same duration of classification as the design information for components. However, this information is still more evolutionary in nature than revolutionary, and information about tactics and strategies no longer in use provides insight into the current tactics. For this reason, the information requires a duration of classification in excess of 25 years. Because its disclosure would reveal information that would assist in the development, production, or use of a WMD, it meets the requirements for exemption from automatic declassification at 25 years. As these strategies evolve over time, no single event will occur that would prevent previous tactics and strategies from revealing sensitive information about tactics and strategies currently in use. It was determined that classifying the information for 50 years should allow enough time for tactics and strategies to change where the older tactics and strategies do not provide insight into the tactics and strategies currently in use.

Recommendations

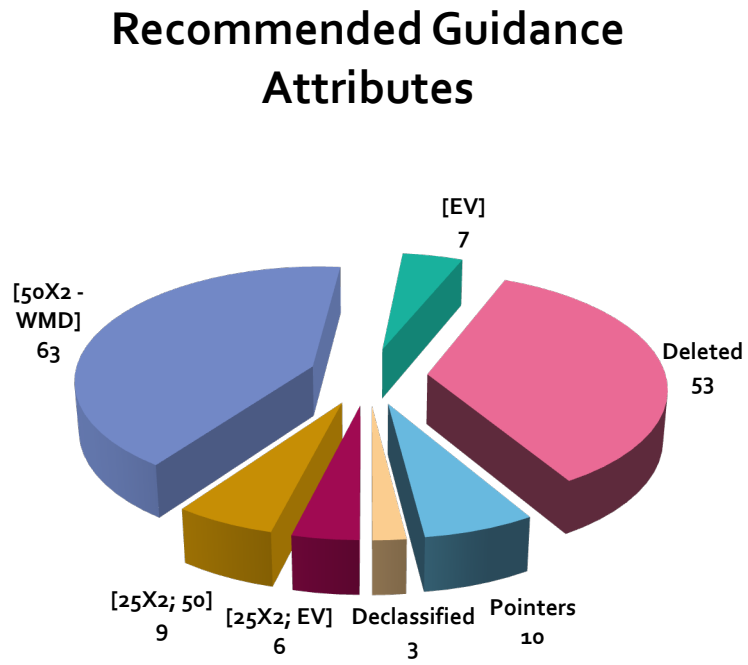
Rewrite the guidance to reflect the classification of the keystones identified. This would result in a reduction in guidance from 152 to 95 topics consisting of the following changes:

- Fifty-two topics would be deleted.
- Three topics would be declassified.
    - One would become unclassified.
    - Two would become UCNI.
- One topic would change from NSI to FRD to correct an error in information equity.
- Ten topics would point to other guidance.
- Sixty-three topics would be exempt from automatic declassification at 50 years.
- Fifteen topics would be exempt from automatic declassification at 25 years.
    - Six of these topics would have a declassification event occur within 50 years of the classification determination.
    - Nine of these topics would be declassified at 50 years.
- Seven topics would be declassified by an event that occurred within 25 years of the classification determination.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 6 - Cyber Security

Current Policy

The current guidance for cyber security addresses the classification of information about an Information Technology (IT) system that makes it possible to gain unauthorized access to the classified information on the IT system. Within the Department of Energy (DOE), IT systems that process classified information provide potentially lucrative targets for compromise. In conjunction with the security measures required by DOE regulations at IT facilities processing classified information, necessary precautions must be taken to protect information pertaining to security measures, where such information might assist a perpetrator in subverting the measures and penetrating the system. Accordingly, the basic principle underlying classification policy for IT system security is to protect information that is of meaningful assistance in gaining unauthorized access to the classified information being processed on an IT system.

Background

The current guidance is contained in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4). The guidance contains 14 National Security Information (NSI) topics related to cyber security information. These topics consist of:

- Nine topics that are declassified after 25 years.
- Three topics with an event driven declassification.
- One topic exempt from automatic declassification at 25 years.
- One topic that refers to other guidance.

The current guidance does not clearly explain how this information assists an outsider in gaining unauthorized access to classified information.

Analysis

Two keystones were identified requiring protection:

- Information that could be exploited by an outside adversary to gain access to classified information on a system.
- Information that reveals a link to a foreign intelligence service.

Application of the first keystone requires defining "could be exploited by an adversary". Classification provides very limited controls on access to the information by an insider (i.e., those associated with an L versus Q clearance). Exploitable does not mean all information that would be useful; rather it is limited to information whose exploitation would clearly result in a national security consequence. While there is a great deal of information that could provide some assistance in gaining access to the information on a classified system, classification of all this information would significantly impair operations and incur substantial costs. Classification is reserved for information that provides significant assistance to an outsider. Other controls, such as designating information Official Use Only, can be applied to information that would be

useful in gaining access, but does not meet the thresholds required to be designated as classified information. Also, classification of a security problem does not mitigate the underlying need to fix the problem. A determination of whether to classify a piece of information requires an assessment by the information owner of the risk assumed in disclosing the information against the cost of protection of the information and the impact on the ability of the Department to meet its mission.

At the time of this report, the Department has not declared any IT systems as mission critical. Because of this, this keystone does not apply to information that would allow an adversary to disable a classified IT system. If, in the future, the Department does declare an IT system as mission critical, an original classification determination will need to be made to classify information that would allow for the disablement of that system.

Because IT systems change significantly in a short time, a maximum classification duration of 10 years was assigned to this information.

Information protected by the second keystone would primarily be the equity of another agency. However, there may be some subset of this information that would be classified by DOE. It includes information identifying the source of a suspected intrusion and countermeasures in place to address these attempts. In addition, because it deals with the identity of the intruder rather than the target, this keystone applies to both classified and unclassified systems.

As these keystones serve as the underlining basis for the classification of information related to cyber security, all the topics in the cyber security guidance should reflect the classification level and duration of these keystones. The topical guidance was then examined to determine how best to apply these keystones to information generated at DOE.

A system-specific password or user generated personal identification number (PIN) code for access to a Department of Energy/National Nuclear Security Administration (NNSA) classified IT system is classified because it is an exploitable element of the security for the IT system. Possession of an authenticator for a DOE/NNSA classified IT system will allow an adversary to reduce the delay time associated with the security for that system provided by the authenticator. While authenticators function as a minor component of security compared to other elements of the security system (the other elements include physical barriers to the classified IT system and encryption technologies that prevent access to the data stream), they are a component of security that can be easily classified to provide some additional control on access to information on the IT system. In a small number of cases, the authenticator is the only barrier to access of the information on the classified IT system. For these few instances, the authenticator requires a higher level of classification to reflect what information possession of the authenticator will provide direct access.

An authenticator cannot be Restricted Data (RD) because, as security information, an authenticator does not meet the definition of RD from the Atomic Energy Act. However, section 8-303 i (1) of DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* dated February 28, 2006, to which DOE is a signatory, requires passwords to be protected at the level and category of the information to which they provide access. This

means, in practice, that while a password may have a lower classification level than the information on the classified IT system, it requires storage and handling commensurate with the level and category of the information on the classified IT system. In addition, the authorization provided by a security clearance to access information of a particular classification level and category does not authorize access to an authenticator that provides access to information of the same classification level and category. Security policies may place additional restrictions, such as limits on the sharing of passwords or PIN codes, independent from the classification.

Information regarding a plan and/or schedule for conducting an upcoming IT system security test (procedures, dates, times, etc.) for the purpose of assessing computer security measures is classified when such knowledge would significantly assist in an attack on a classified IT system. Because classification does not provide a significant barrier to access of the information by an insider, this information must significantly assist an outside adversary in an attack in order to be classified. Information about a completed test is classified when this information can be used to determine exploitable information about a future test.

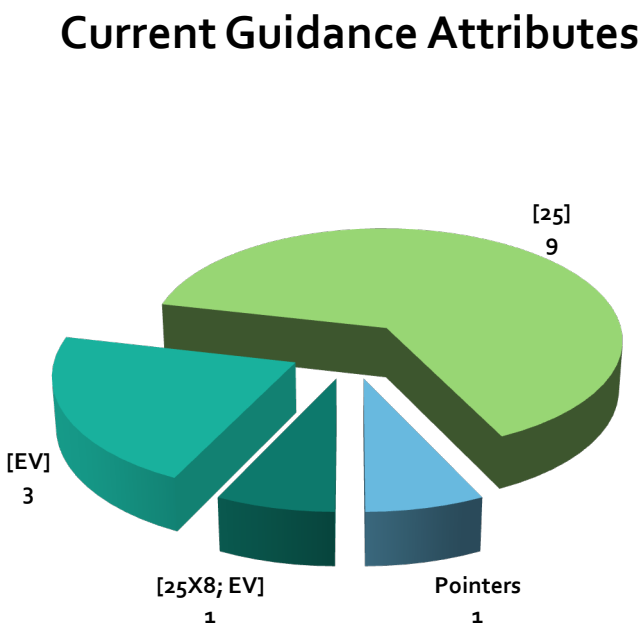
Information about methods to circumvent existing hardware and supporting software that provides security for a classified network is owned by the NSA and should be referred to that agency for classification determinations.

Recommendations

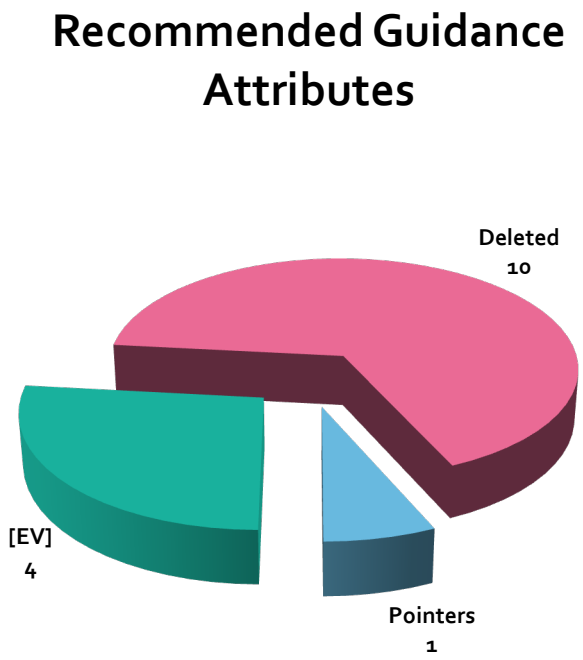
Rewrite the guidance to reflect the classification of the keystones. In addition, clarify throughout the guidance that while authenticators cannot be classified RD, they will be protected as such in accordance with the NISPOM. Topics should be added to refer information that reveals a link to a foreign intelligence service to the cognizant counterintelligence organizations. This would result in the following changes in guidance:

- 10 topics would be eliminated because of redundancy.
- 2 topics would be changed from a 25-year duration to an event or 10 years, whichever occurs first.
- 1 topic would replace 2 classification determinations with instructions to refer the information to another agency.

The following chart identifies the declassification instructions used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 7 - Information Security

Current Policy

Five sections of *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4) contain topics that address non-Information Technology information security. These sections are titled Incidents of Security Concern, Protection Program Operations, Classification Change Notices, Operations Security, and Nuclear Material Control and Accountability. These topics address the classification of compromise information, information related to investigations of security incidents, the loss of classified matter, combinations, classification change notices, operational security assessments, and the fact of a missing item of SNM. In some cases, it is not clear how the information classified by these topics would cause damage to national security if disclosed. Other topics seem to identify some information as NSI that should be protected as Restricted Data or Formerly Restricted Data.

Background

The topics in the Incidents of Security Concern section attempt to address the classification of all information generated in the inquiry into a security incident. The section begins with topics covering the classification of compromises that occur by e-mail or other electronic means. It then moves to the classification of FBI involvement in an investigation at a DOE facility. The section also contains topics for missing classified matter and compromises of classified information. These topics consist of:

- Nine exempt from automatic declassification at 25 years.
- Ten with an event driven classification.
- One that points to other guidance.

In the Protection Program Operations section, one topic classifies combination and codes. This topic classifies a combination or code at the level and category of the information to which the combination or code provides access. A note to the topic instructs that a combination or code be designated at the highest level, category, and access caveats associated with the material in the security container. This topic has an event driven declassification. Four topics in this section classify the fact of an attempted theft or diversion of a nuclear weapon or SNM of a certain quantity or greater. Three of these topics have an event driven declassification. One is exempt from automatic declassification at 25 years.

The section titled, Classification Change Notices contains three topics that point to other guidance. The remaining topic classifies change notices until all the classified matter has been upgraded and there is a reasonably certainty that no compromise occurs. This topic is exempt from automatic declassification at 25 years.

In the Operations Security section, the topics classify information related to an operations security (OPSEC) assessment (OA). This includes statements of the threat, descriptions of OPSEC procedures, methods to defeat countermeasures, OA planning information, OA results, critical program information, and indicators. These topics consist of:

- Seven exempt from automatic declassification at 25 years.
- One that is declassified at 10 years.
- Seven with an event driven declassification.
- Five that point to other guidance.

The section titled Nuclear Material Control and Accountability contains four topics that address the fact of a missing item of SNM. Two of these topics are exempt from automatic declassification at 25 years. The remaining two topics have an event driven declassification.

Analysis

The following three keystones were identified for the information:

- Information that would assist an adversary in acquiring classified information.
- Information that would assist an adversary in acquiring material (SNM, a weapon, a part).
- Information that can damage foreign relations.

When DOE or a DOE contractor cannot account for either SNM or a classified document (i.e., any medium that conveys classified information, such as printed matter, an e-mail, a CD-ROM, or a hard drive), meaning that it is not immediately known what happened to the SNM or classified document, a search is initiated. If the search fails to locate the SNM or classified document or there is evidence to suggest theft, the Federal Bureau of Investigation (FBI) is notified and provided an opportunity to conduct an investigation.

The FBI may classify the fact of their involvement in an investigation at a specific site or facility. The FBI may also classify details of the investigation. Once FBI involvement begins, FBI classifies information about the investigation and that agency should be contacted for guidance. At the conclusion of the investigation or if the FBI chooses not to conduct an investigation, the Office of Classification should be contacted to determine if any unique information regarding the incident requires classification. This could include information that was classified by the FBI during but not after completion of the investigation. It could also include information that is still classified by the FBI where it has been determined a separate DOE equity exists. In any case, specific classification guidance for the incident will be generated either during or after the completion of the FBI investigation.

In the event of a suspected overt theft, the Emergency Operations Center (EOC) and the Tactical Operations Center (TOC) at the site would be activated. The protective force staffs the TOC, which supports the security incident commander (IC) in tactical matters. The TOC serves as the primary focal point for the security IC and the point of contact for outside law enforcement agencies. The EOC coordinates between the incident commander and the site manager, the individual in charge of coordination of site/facility response activities.

During the theft, the IC determines how information will be controlled. This includes what information can be transmitted over unencrypted radios and what information can be shared with local law enforcement. The IC bases these determinations on assumptions of what the target of

the theft is and a judgment that release of the information will assist in disruption of the suspected theft or the recapture or recovery of the stolen matter. After disruption of the theft or recapture or recovery of the matter, the site manager determines what information to release about the incident to local law enforcement and the local government through the EOC.

If, after the incident, there is a decision to classify information related to the theft, the information released by the IC and the site manager will be examined to determine whether in can be returned to Government control. An original classification authority will decide what information to classify related to an incident based on the results of this examination.

When given a piece of classified foreign government information (FGI), the Government agrees to protect the information in the same manner as U.S. classified information of an equivalent level. As the disclosure that the U.S. Government may have mishandled specific FGI could cause damage to foreign relations, particularly with the foreign government whose information may have been compromised, the fact that FGI belonging to a specified country cannot be accounted for is classified. Any information that identifies a specific classified document as unaccounted for when that document contains FGI is classified.

A determination that a classified document is missing occurs after the Government has concluded there was no act of theft and has performed an exhaustive search with the assistance of other agencies and local and state law enforcement of all potential locations of the document. As the resources of the Government were not able to locate the document with all available information, it is not credible for an adversary to locate the document with the same information. Because of this, most of the information about a document determined to be missing is not classified.

Information that significantly assists an adversary in locating classified information in the open literature or public domain (such as a web site, book, or a periodical) where the information is immediately available and there is no Government restriction to accessing the information is classified. Once the information contained in a document has been compromised, placing the document back under Government security controls does not recover the information. If the Government is unable to re-control the information through a mechanism such as a nondisclosure agreement, information that allows an adversary to locate the document, including information that identifies the document, is classified.

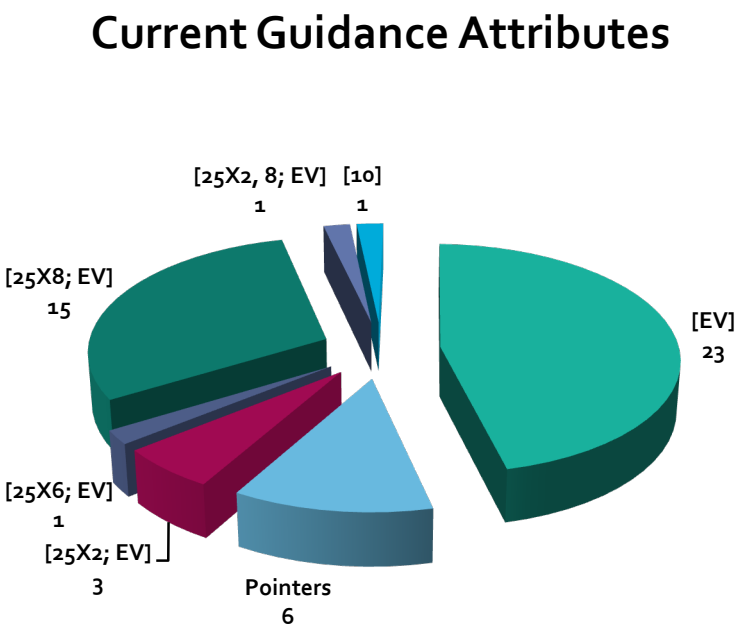
Combinations for security container locks that contain classified information are classified at the level of the information inside the container. Combinations cannot be RD or FRD as combinations are security components and do not meet the definition for RD or FRD in the Atomic Energy Act. The determination to protect the information at the level of the information inside the container comes from the National Industrial Security Program Operating Manual (NISPOM) to which the DOE is a signatory. See section 5-308 of the NISPOM for details. The NISPOM does not contain protection requirements for SNM, but the combinations for security containers that contain a Category I or II quantity of SNM are classified to limit dissemination of the combination between employees at the facility.

Recommendations

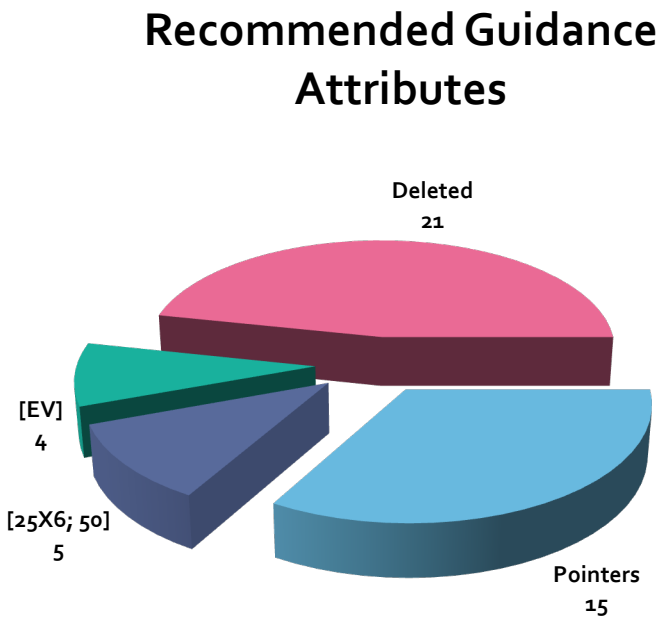
Rewrite the guidance to reflect the working group analysis. These changes results in new guidance that contains 29 NSI topics. The topics consist of the following:

- Twenty-one topics will be deleted.
- Six topics will be exempt from automatic declassification at 25 years.
- Five will have an event driven declassification.
- Eighteen will point to other guidance.

The following chart identifies the declassification instructions used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 8 - TEMPEST, COMSEC, and Cryptology

Current Policy

Communications security (COMSEC) is the measures and controls taken to deny unauthorized individuals information derived from telecommunications while ensuring the authenticity of such telecommunications. These measures include TEMPEST, a short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment, and cryptology, the science and study of codes and cipher systems. With the introduction of Secure Terminal Equipment (STE) in government, the Atomic Energy Commission (AEC), the predecessor agency to the Department of Energy (DOE), developed classification guidance with the concurrence of the National Security Agency (NSA), the owners of the STE information. The current guidance for TEMPEST, COMSEC, and Cryptology Information provides classification guidance for the protective measures in place to deny unauthorized individuals information derived from telecommunications of the U.S. Government that is related to national security.

Background

In 1985, DOE decided to combine a variety of safeguards and security classification guidance into a single document entitled, "CG-SS-1, Safeguards and Security Classification Guide". The topics from the STE guidance were updated and coordinated with NSA before being incorporated as a chapter in this guide. CG-SS-1 has been updated several times since 1985 and is now the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), change 6.

CG-SS-4 contains 102 topics that address the classification of TEMPEST, COMSEC, and Cryptology Information. These topics consist of:

- Thirty-five topics exempt from automatic declassification at 25 years that are declassified at 50 years.
- Fifty-three topics exempt from automatic declassification at 25 years with an event driven declassification.
- One topic with an event driven declassification.
- Thirteen topics that point to other guidance.

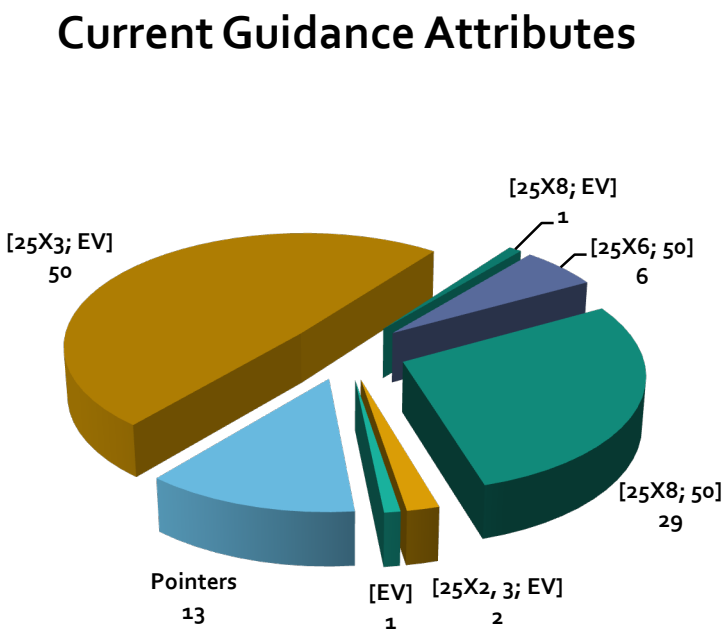
Analysis

The NSA, the equity owner for COMSEC information, reviewed the guidance in CG-SS-4 as part of that agency's FCGR activities. They recommended removing the topics from DOE guidance as they have made their classification guides available electronically.

Recommendations

- Remove the topics from DOE guidance in accordance with the NSA recommendation.

The following chart identifies the declassification instructions used in the current guidance:



Working Group 9 - Material Control and Accountability

Current Policy

As part of its responsibilities under the Atomic Energy Act of 1954, as amended, the Department of Energy (DOE) maintains inventories of Special Nuclear Materials (SNM) required to execute various national security missions. These materials are difficult to obtain and are required to build several types of weapons of mass destruction (WMD). The U.S. Government considers proper control and accounting of these materials to be an important aspect of proliferation prevention efforts. DOE operates a Nuclear Material Control and Accountability (MC&A) program to ensure this is accomplished. Certain MC&A information could provide significant assistance to persons or organizations attempting to obtain special nuclear material (SNM) for unauthorized uses. It is the policy of the U.S. Government to classify this information to prevent damage to national security. DOE provides classification guidance for this information in *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4).

Background

The guidance in CG-SS-4 for MC&A contains 57 National Security Information (NSI) topics. The topics cover inventory quantities, accounting capabilities, physical control of SNM, deficiencies in program performance, and methods/techniques to defeat systems. These topics consist of:

- Four that are declassified after an event occurs.
- Seven that are exempt from automatic declassification at 25 years.
- Forty-six that refer to other classification guidance.

Analysis

The working group identified five NSI keystone concepts as requiring protection in order to ensure the proper safeguarding and security of SNM inventories. These keystones are:

- Diversion Detection Threshold – Identification of the quantity that can be diverted without detection from a SNM inventory.
- Targeting Information – Assists the adversary in selection, targeting, or timing of an attack against an asset.
- Deficient Performance – Determined by the Officially Designated Federal Security Authority or Officially Designated Security Authority, performance less than that required for the protection system to function at design effectiveness.
- Exploitable Design Information – Adversary exploitation of its design or operational characteristics would lower expected performance of a DOE developed or modified security element/component.
- Novel Method/Technique – a DOE developed method/technique that defeats or degrades performance/functioning of a security element/component.

The bulk of classified information generated by MC&A programs is used to determine the diversion detection threshold, as well as for computing deviations from expected inventory quantities. Currently all measurements that make up an inventory and the associated analyses is classified CNSI and exempted under 25X2. The data meets classification requirements only when all the measurements for an inventory activity are consolidated and the analyses are performed to calculate the diversion detection threshold. All individual measurements should be treated as unclassified. The ability of installed measurement systems in DOE facilities to detect diversion is not improving significantly over time, so in some cases data from over 50 years ago can potentially aid in planning a diversion attempt. The compiled measurement data sets and calculated diversion detection thresholds are more correctly classified as CNSI 50X2-WMD when the information can aid a diversion attempt on a measurement system currently in service. Similar to limitations on the ability to measure a quantity of SNM, there is an inability to exactly calculate or measure the amount of holdup that accumulates in a material processing operation, such as a plutonium purification process. Knowledge of holdup uncertainty values could aid in the selection of a desirable target for diversion activities. The value of this information is considered to be similar to knowledge of measurement diversion detection thresholds, so a classification of CNSI 50X2-WMD is considered appropriate when the information aids a diversion attempt on a process that is in service.

The existing topics related to system deficiencies and diversion scenarios do not clearly identify who determines if a deficiency exists or at what classification level it should be protected. It is helpful to the derivative classifiers using the guidance if the security personnel responsible for declaring deficiencies and viable diversion scenarios are identified, by position. Because it was determined to only damage national security, per Executive Order 13526, Sec. 1.2, deficiency and diversion scenario information should be protected as confidential, not secret.

Additional MC&A specific guidance is needed concerning exploitable design information regarding DOE designed or modified equipment used in SNM protection systems, as the current guidance contains no topics that address MC&A related security equipment. Such guidance would be appropriately classified as CNSI 25X2.

Another area that was identified as containing equities currently approaching or passing 50 years of age involves methods for defeating Tamper Indicating Devices (TIDs). The department uses various types of TIDs to secure containers, vaults, and security equipment used to protect SNM. Some of these TID designs are now over 50 years old and DOE developed techniques for surreptitious defeat of these devices must be protected to maintain the effectiveness of these devices.

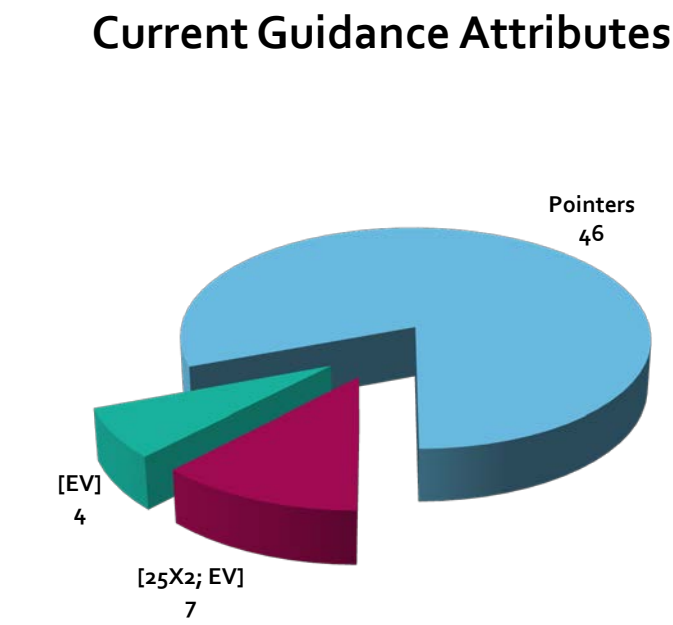
Recommendations

The guidance should be rewritten to reflect the following recommendations of the working group. The revised topic language improves the usability and correctness of MC&A related topics.

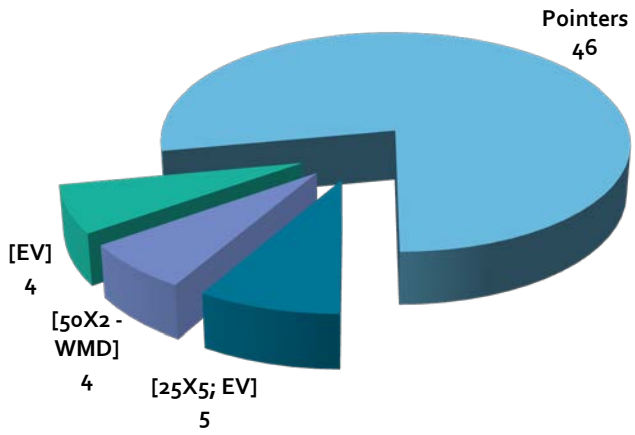
- Clarify that diversion detection thresholds are only classified for Category I/II quantities (or for credible rollup scenarios) in active/processing inventories.

- Exempt the diversion detection thresholds for Category I/II quantities in active/processing inventories from automatic declassification under 50X2-WMD.
- Classify holdup calculation uncertainty values when they exceed a Category II quantity and exempt from automatic declassification under 50X2-WMD.
- Clarify who declares credible MC&A deficiencies and diversion scenarios (by position).

The following charts identify the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 10- Graded Security Protection

Current Policy

The current guidance for Graded Security Protection (GSP) encompasses information related to the protection of vital assets at DOE sites and facilities. The GSP Policy revised the performance basis for the Department of Energy's (DOE) security guidelines, replacing the Design Basis Threat (DBT) Policy in August 2008.

DOE protection programs are required to provide effective protection against credible malevolent attacks and other hostile actions against a broad range of national security assets. DOE policy further requires a performance-based approach demonstrating protection effectiveness. Because DOE resources are limited, higher levels of protection and different protection strategies are implemented for assets of greater national security concern. DOE policy mandates a graded protection, risk management approach to meeting policy requirements. DOE "recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential consequences of all malevolent events to zero.)" The GSP Policy further directs that a graded approach be followed, in which the highest investment of security resources be apportioned in a manner to provide protection to those assets whose "loss, theft, compromise, and/or unauthorized use" would most seriously affect national security. Protection of other interests and activities must be graded accordingly. Provision at every asset level is also made for informed acceptance of risk by the appropriate level of management. The GSP provides the framework for long-term security system design based upon a stable and sustainable set of performance metrics. **It** is the standard for measuring the effectiveness of installed security measures. GSP has explicitly implemented concepts intended to ensure a balanced risk management foundation for security system planning in a resource-sensitive environment. Part of this risk management is the use of classification to protect those details about DOE protection planning that would assist significantly a DOE adversary in devising and executing a successful attack on a DOE facility, resulting in damage to national security.

Background

The GSP prescribes the protection requirements for the following assets at DOE facilities: nuclear weapons, nuclear components, and nuclear test devices in DOE custody; Special Nuclear Material (SNM) of improvised nuclear device (IND) concern; SNM of theft concern; nuclear, chemical, and biological materials of a public and employee health and safety concern; critical national security facilities and assets designated by DOE, such as the Bonneville Power Administration; and classified information and matter.

The implementation of a performance and risk management based security system requires the designation of assets to be protected, in descending order of consequence, and the identification of a policy-defined set of adversary capabilities, against which each level of asset must be protected. The definition of adversary capabilities includes specification of characteristics such as adversary team size, available weapons and equipment, extent of target knowledge and access attributes, and tactical/technical skills. A key element for defining adversary capabilities is the available threat intelligence, usually expressed as a range of numbers and capabilities rather than a single set. The graded protection approach categorizes all assets into one of five levels based

on the general consequence of loss, destruction, or impact to public health and safety at a facility or the program, project, or activity conducted.

The GSP identifies and characterizes potential adversary threats to DOE assets. Adversary types are defined in terms of characteristics and potential capabilities. Adversary types include terrorists, individual criminals, organized criminals, psychotics, disgruntled employees, violent activists, intelligence collectors, and insiders. Protection strategies are defined for each type of asset in a DOE facility based on adversary type and team size. The most sensitive information contained in the GSP relates to the most capable adversary, which is a terrorist team. Several types of equipment and capabilities associated with this adversary type are classified by current guidance.

Current DOE guidance for GSP information, consisting of a total of 41 topics, is found in *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), *Annex to Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4A), and *Supplemental Guidance for the Graded Security Protection Policy* (TNP-37). These topics consist of:

- Twenty-seven topics exempt from automatic declassification at 25 years with event based declassification instructions.
- Twelve topics to be declassified after 25 years.
- Two topics that point to other guidance.

After removing the pointers, the remaining 39 topics were examined.

Analysis

Identified the following proposed keystones for GSP information:

- Intelligence Sourced Capability – Inclusion or exclusion of an adversary characteristic/capability is based on and would reveal intelligence collection, analysis, or an assessment classified by DOE or, more likely, by another Intelligence Community (IC) agency. The declassification event is when the intelligence information is declassified; therefore, 25X1 applies. Because an intelligence sourced capability is unlikely to allow the identification of a human intelligence source, 50Xl-HUM is unlikely to apply.
- Requirement Deficiency – Determination that a facility cannot meet a GSP protection requirement for a specific asset. Assists adversary attack optimization by exploitation of deficiency. Because neither the GSP requirements, the GSP adversary characteristics, the facility installed physical security systems, nor the protective force capabilities and planned response remain static, declassification at 25 years is appropriate.
- IND Information- Non-RD information about improvised nuclear devices (INDs) used in VA scenarios. This information is SNSI under EO 13526 (h) and exempt under 50X2-WMD.
- Four other keystones concerning adversary capabilities whose descriptions are classified. A 25X2 exemption may apply to a specified adversary under these keystones, if exploitation of the information would lead to potential national security consequences.

The 25X1 exempted topic in CG-SS-4 refers to the DBT for additional details. These "details" in the DBT, which were carried forward to the GSP, do not meet the requirement for this exemption. Classification may still be warranted, but if so it would have a stronger basis under a different keystone adversary capability with a 25X2 exemption.

The 25X2 exempted GSP topic in CG-SS-4 is unnecessary because it addresses information not used in vulnerability assessments under the GSP. The one topic under this exemption in CG-SS-4A was determined to likely meet the requirement for a 50-year exemption as WMD key design information. The 16 topics in TNP-37 under this exemption were based on the physical security vulnerability classification. Classification and declassification of this information was analyzed in Working Group 1, Security Vulnerabilities. The proposed declassification for this information is 25 years with no exemption. **It** is identified here under the requirement deficiency keystone.

The eight 25X8 exempted topics and 12 topics declassified at 25 years all address adversary capabilities and characteristics (e.g., adversary numbers, allowed equipment/weapons, etc.). The generic capabilities identified in most of the 25X8 exempted topics are not specific enough for a derivative classifier (DC) to apply to the specific, detailed descriptions of adversary capabilities now found in the GSP and associated documents. The 25-year declassification topics are specific enough for use, but the declassification at 25 years was found to be in error because these specified capabilities will likely remain amongst assumed adversary capabilities and exploitation will continue to result in expected damage to national security for longer than 25 years.

Because almost all DOE assets addressed by the GSP would assist in the development, acquisition, or use of WMD (SNM, nuclear weapons, RD information (nuclear weapon design, nuclear material production technology, etc.)), the proper exemptions should be 25Xl for any Intelligence Sourced Capability and 25X2 for capabilities under any of the other proposed capability keystones. The declassification for an intelligence sourced capability occurs when the underlying intelligence is declassified. The declassification for other capabilities is the program office determination for the GSP that the capability no longer meets the conditions of its keystone.

Overall, the current guidance does not provide a DC with enough information to make proper classification determinations. Adversary characteristics, capabilities, and requirements, and the GSP policy itself are spread over three documents and frequently change.

Recommendations

- To consolidate all GSP classification guidance in one guide, CG-GSP-1.
- To only exempt specified adversary capabilities from automatic classification under 50X2-WMD on a case-by-case basis.
- For all other adversary capabilities and characteristics, to only classify, by topic, keystone capabilities.
- To require the policy office responsible for the GSP to maintain an adversary capabilities list with each specific adversary capability uniformly classified with GSP adversary capabilities keystone topics.

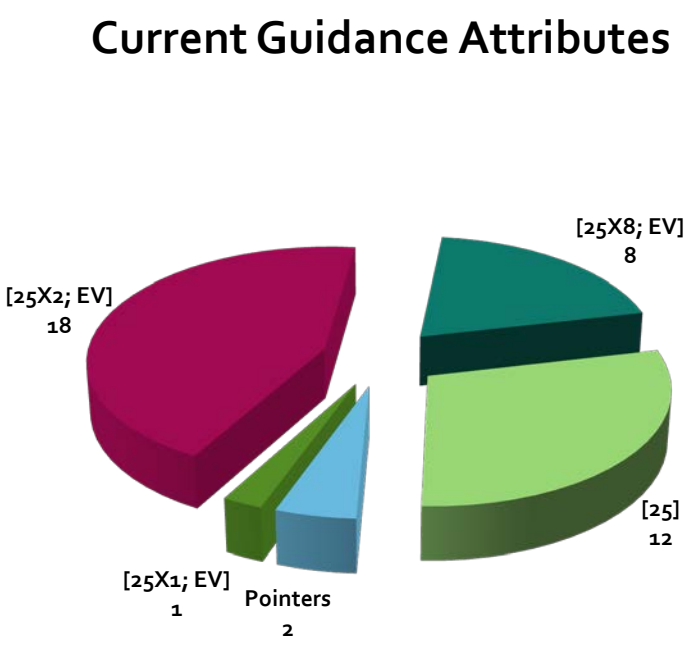
- To reduce duration of classification for information meeting the requirement deficiency keystone to no more than 25 years because neither the GSP requirements, the GSP adversary characteristics, the facility installed physical security systems, nor the protective force capabilities and planned response remain static. Exceptional cases will be handled with specific original classifications.

This would result in the following:

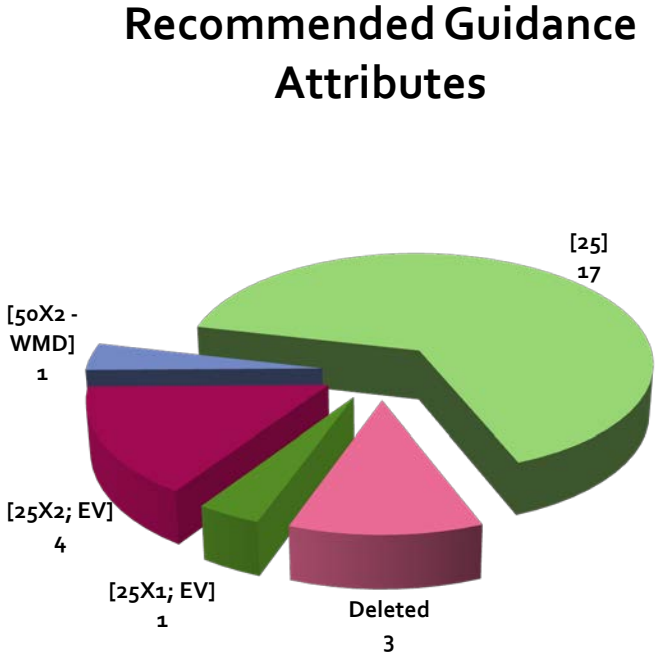
- One 25X2 exempted topic for non-RD information about INDs changed to a 50X2-WMD exemption.
- No 50X2-WMD topics for specified adversary capabilities (GSP policy office has not identified any capabilities requiring this).
- Eight 25X8 exempted, one 25X2 exempted, one 25Xl exempted, and twelve 25-year declassification topics replaced with one 25Xl exempted keystone and four 25X2 exempted keystone capability topics.
- One 25X2 exempted topic deleted.
- Added a 25-year declassification topic for the requirement deficiency keystone.
- Sixteen 25X2 exempted topics (all identified as requirement deficiencies) changed to declassified at 25 years.
- Two pointer topics deleted (better addressed by a note or caution).

The number of classification topics would be reduced from 41 topics to 23 topics. Of these only five topics will be exempted from automatic declassification at 25 years.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 11a – Intelligence

Current Policy

Executive Order (E.O.) 12333, *United States Intelligence Activities*, assigns to the Department of Energy (DOE) certain responsibilities in the areas of intelligence (IN). DOE does not covertly collect intelligence information, though it does use and analyze intelligence information covertly collected by other agencies in the Intelligence Community (IC). It overtly collects intelligence information on foreign energy matters. It produces and disseminates, with DOE, foreign political, economic, military, or facility threat-related intelligence information. It manages, coordinates, and oversees the production of foreign scientific and technical intelligence relating to nuclear proliferation, nuclear weapons, energy, and threat-related and emerging nuclear technologies in support of DOE and the IC. DOE provides expert technical, analytical and research assistance to other agencies in the IC, conducting analyses of both open source information and intelligence information collected by other U.S. Government (USG) agencies. DOE analyses of foreign nuclear programs typically use Restricted Data (RD); the results of these analyses are RD, and guidance in this area is outside the scope and purview of this fundamental review.

Transclassified Foreign Nuclear Information (TFNI) is intelligence information concerning the atomic energy programs of other nations that was RD but has been removed from the RD category under an agreement between DOE and Director of National Intelligence (DNI). This transclassification was formalized under E.O. 13526 and is exempt from automatic declassification.

Background

DOE classification guidance for derivative classifiers (DC) in DOE intelligence program information (a total of 73 topics) is found in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), the *Annex to Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4A), and the *DOE Classification Guide for Intelligence Information* (CG-IN-1).

The current National Security Information (NSI) intelligence topics consist of the following:

- One topic exempt from automatic declassification at 25 years because the release would impair the effectiveness of an intelligence method currently in use, available for use, or under development (25X1).
- Four topics exempt from automatic declassification at 25 years because the release would reveal the identity of other IC agency human sources (25X1-human).
- Fifteen topics exempt from automatic declassification at 25 years because the release would reveal a relationship with an intelligence or security service of a foreign government (FG) or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development, or reveal information that would cause serious harm to relations between the U.S. and a FG, or to ongoing diplomatic activities of the U.S. (25X1,6).

- One topic exempt from automatic declassification at 25 years because the release would reveal information that would cause serious harm to relations between the U.S. and a FG, or to ongoing diplomatic activities of the U.S. (25X6).
- One topic exempt from automatic declassification at 25 years because the release would reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security (25X8).
- Eighteen topics that are declassified at 25 years.
- Five topics with an event-driven declassification.
- Twenty-one topics that point to other guidance.
- Seven topics that refer to another IC agency, the Director of Central Intelligence, or Federal Bureau of Investigation for declassification.

Analysis

Identified the following three keystones for IN:

- Two keystones whose descriptions are classified and which would require referral to other Government agencies following declassification of DOE's equity.
- TFNI Identification – Raw foreign nuclear intelligence information for which comparable U.S. information is RD. Any analysis or confirmation of TFNI that uses or reveals RD is RD. This keystone is completely exempt from automatic declassification. It may not be declassified until DOE declassifies the corresponding RD information. The information may remain classified for other reasons as determined by IC agencies.

Many of the topics provide instructions for other IC agency equities. Since these classification guides are not joint guides with other agencies, other agency classified information is better addressed in notes or cautions to topics.

The conditions identified in most of the IN topics are not specific enough for a DC to apply consistently. In attempting to address information that has many unique facets that would or would not make it classified with broad topics, the existing guidance inadvertently places the DC in the position of determining the level of damage caused to national security by the release of the information. In addition, the information covered by the topics generally falls under the cognizance of additional agencies in the IC. If DOE were to generate specific information that met the conditions in these topics and damage national security, an original classification authority for IN should classify the information under E.O. 13526 1.4 (c), which would then be the basis for new derivative classification guidance.

Additional original classification authorities have been granted to key personnel in the DOE Office of Intelligence. Per DOE Order 475.2A, *Identifying Classified Information*, DCs who identify information that they believe damages national security will protect it as classified and submit it to an original classifier (OC) for an original classification determination. These original determinations will be collected in either a classification bulletin, a specific program classification guide, or as a change to the DOE overall intelligence program guide (CG-IN-1).

All intelligence guidance in CG-SS-4 and CG-SS-4A was determined to duplicate guidance in CG-IN-1. This guidance was intended to serve as a bridge between safeguards and security and intelligence. However, DCs in security, while possessing the authority to use CG-SS-4A and, therefore, the authority to derivatively classify IN information, did not have the expertise to consistently apply the guidance appropriately. It is better for a DC in security to protect as classified any information that broadly falls under intelligence and refer it to a DC with the appropriate authorities for DOE intelligence information. In practice, this is what has been happening.

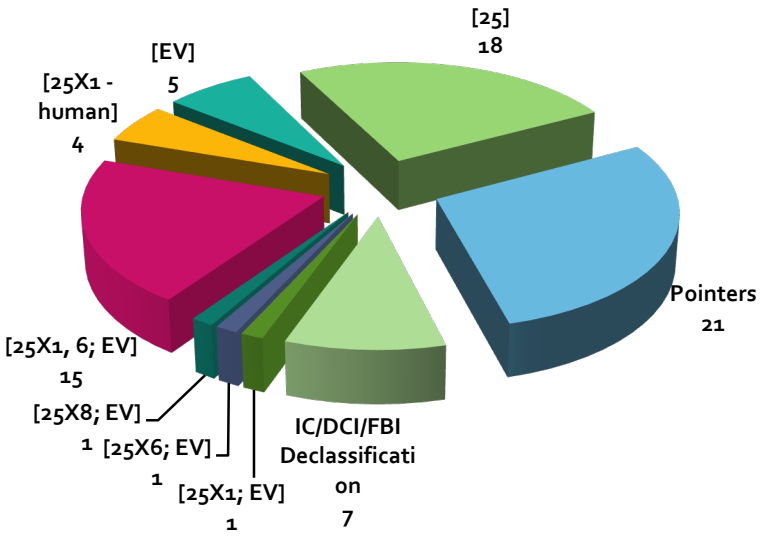
Some DOE IN budget information is classified because it is classified by the DNI or other IC agencies funding DOE IN activities. The overall DOE IN budget is classified by the DNI. This is fairly explicit and to remain compliant with this DNI classification, a topic will be retained in the IN guidance. The current topics classifying some other budget information are not specific enough for DC use. They should be deleted. Budget information concerning specific programs that is determined to reveal classified information about sensitive IN programs will be handled with specific original classification determinations.

Recommendations

- Delete the three IN topics in CG-SS-4 and the one IN topic (points to CG-IN-1) in CG-SS-4A and replace with a summary of intelligence guidance in CG-SS-4 or its successor.
- Delete the forty IN topics that either are not specific enough for DC use, require the DC to exercise OC judgments, or point to other agency guidance or source documents for classification and declassification.
- Delete twenty-one topics about Sensitive Compartmented Information Facility (SCIF) security (already covered by safeguards and security guidance).
- Delete four other agency human source topics because this is not a DOE equity.
- Add two keystone topics whose descriptions are classified.
- Add a keystone topic for TFNI Identification.
- Retain the overall IN budget classification topic with declassification instruction for referral to DNI with the DOE equity declassified at 25 years.

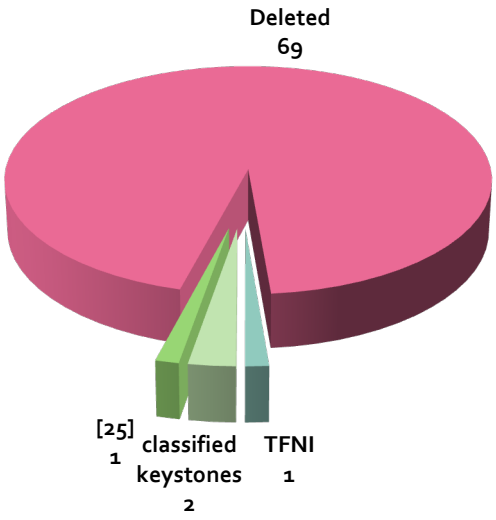
These recommendations would result in only four classified topics.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:

Recommended Guidance Attributes



Working Group 11b – Counterintelligence

Current Policy

Executive Order (E.O. 12333, *United States Intelligence Activities*, assigns to the Department of Energy (DOE) certain responsibilities in the areas of counterintelligence (CI). DOE produces and disseminates, within DOE, foreign political, economic, military, or facility threat-related CI information. It conducts CI activities to protect DOE information, personnel, and assets from international terrorist actions and from intelligence collection on the behalf of foreign powers or entities. DOE CI activities are required to detect and deter insiders who act on behalf of a foreign intelligence service (FIS) or international terrorist entity.

Background

DOE classification guidance for derivative classifiers in DOE counterintelligence program information (a total of 144 topics) is found in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), the *Annex to Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4A), and the *DOE Classification Guide for Counterintelligence Informatio*n (CG-CI-1).

The current CI topics (144 in total) consist of the following:

- Seventy-nine topics exempt from automatic declassification at 25 years because the release would reveal a relationship with an intelligence or security service of a foreign government or international organization, or the use of a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development with 75 of the topics referring declassification to the Federal Bureau of Investigation (FBI), Director of Central Intelligence (DCI), other Intelligence Community agency, or by source document (25X1).
- Six topics exempt from automatic declassification at 25 years because the release would reveal the identity of other IC agency confidential human sources or a human intelligence sources (25X1-human).
- Five topics exempt from automatic declassification at 25 years because the release would reveal a relationship with an intelligence or security service of a foreign government or international organization, or the use of a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development; or reveal information that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States (25X1,6).
- Two topics exempt from automatic declassification at 25 years because the release would reveal information that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S. (25X6).
- Six topics in CG-SS-4 exempt from automatic declassification at 25 years because the release would reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security (25X8).
- Eighteen topics that are declassified after 10 years or at 25 years.
- Fourteen topics with an event-driven declassification or point to other guidance.

- Fourteen topics with declassification determined by DOE or another IC agency.

Analysis

Identified the following six keystones:

- Three keystones whose descriptions are classified.
- Source Identification – Information from and/or the identity of individuals whose disclosures of information put them at risk of retaliation, including endangering the lives of the individuals, their friends, or family. This keystone ensures that DOE abides by Director of National Intelligence (DNI) policy to protect IC agency sources by classifying any DOE generated information that could reveal them. Any DOE information that allows the identification of other IC agency sources is classified under E.O. 13526 1.4 (c) and DOE will exempt from automatic declassification under 50X1-HUM.
- CI Identification – Information that identifies or describes the specific activities or indicators of an FIS agent or a DOE employee acting on the behalf of an FIS. This is a joint equity between DOE and FBI. The DOE equity is classified under E.O. 13526 1.4 (c). This information may be exempted by DOE from automatic declassification under 25X1 for 50 years, though specific information may be declassified far earlier, dependent on the particular circumstances, such as the need by the FBI for the information to be disclosed pursuant to an espionage prosecution.
- Exploitable Design Information – Adversary exploitation would lower expected performance of a DOE developed or modified element/component. Because this is used for CI activities, E.O. 13526 1.4 (c) applies and may be exempted from automatic declassification at 25 years under 25X1 because it would impair the effectiveness of an intelligence method currently in use.

Most of the CI topics address information for which DOE shares equity with other IC agencies or organizations, primarily FBI. None of these classification guides is a joint guide. Because these are DOE only guides, information that is solely classified by another IC agency should not be classified by DOE topical guidance. Concerns about other agency classified information are better addressed in notes or cautions to topics.

The conditions identified in many of the CI topics are too broad for a derivative classifier to apply consistently. In attempting to address information that has many unique facets that would or would not make it classified, these topics inadvertently place the DC in the position of determining the level of damage caused to national security by the release of the information. In addition, the information generally falls under the cognizance of additional agencies in the IC. Rather than retaining these broad topics, a DOE original classification authority (OCA) for CI should classify specific information about a DOE CI method, source, or activity that meets the requirements for classification (demonstrable damage to national security, etc.); this original classification will then be the basis for DOE derivative classification guidance for that specific information.

Additional original classification authorities have been granted to key personnel in the DOE Office of Intelligence and Counterintelligence. Per DOE Order 475.2A, *Identifying Classified*

Information, DCs who identify information that they believe damages national security will protect it as classified and submit it to an OCA for an original classification determination. These original determinations will be collected in either a classification bulletin, a specific program classification guide, or as a change to the overall DOE CI program guide (CG-CI-1 or its successor).

Much CI information, particularly that associated with investigations and inquiries, may be joint equities with the FBI. Many of the decisions about classification and declassification are, by necessity, case-specific. Rather than attempting to provide broad classification guidance for DC use and to specific CI cases, it was determined that DOE guidance should instruct the DC to protect information as Secret National Security Information pending an original classification determination by a DOE OCA.

All CI guidance in CG-SS-4 and CG-SS-4A was determined to duplicate guidance in CG-CI-1. This guidance was intended to serve as a bridge between safeguards and security and CI. However, DCs in security, while possessing the authority to use CG-SS-4A and, therefore, the authority to derivatively classify CI information, do not have the expertise to consistently and appropriately apply the guidance. It is better for a DC in security to protect as classified any information that broadly falls under CI and refer to a DC with the appropriate authorities and expertise for classification. In practice, this is what has been happening.

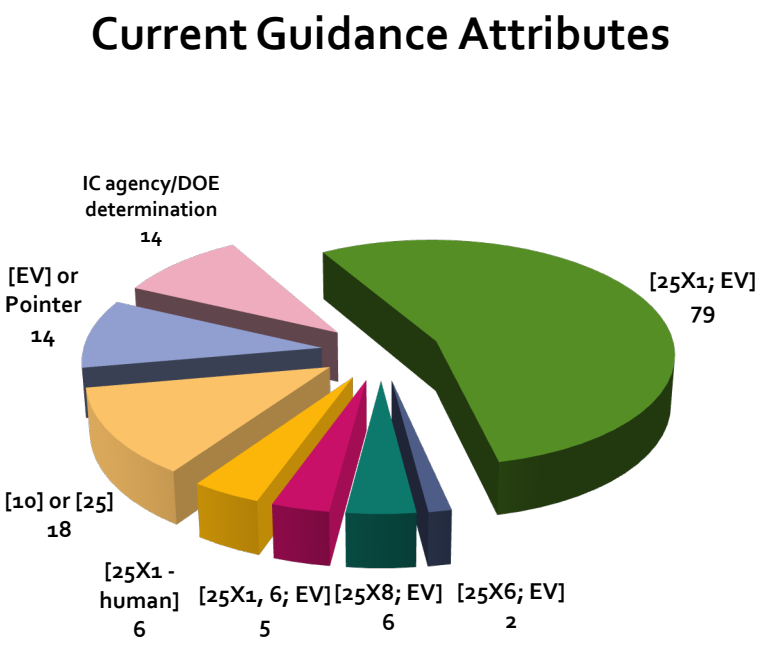
Some DOE CI budget information is classified because it is classified by the DNI or other IC agencies funding DOE CI activities. The overall DOE CI budget is classified by the DNI. This is fairly explicit and to remain compliant with this DNI classification requirement, a topic will be retained in CI guidance. The current topics classifying some other budgeting information are not specific enough for DC use. Budget information concerning specific programs that is determined to reveal classified information about sensitive CI programs is better handled with specific original classification determinations.

Recommendations

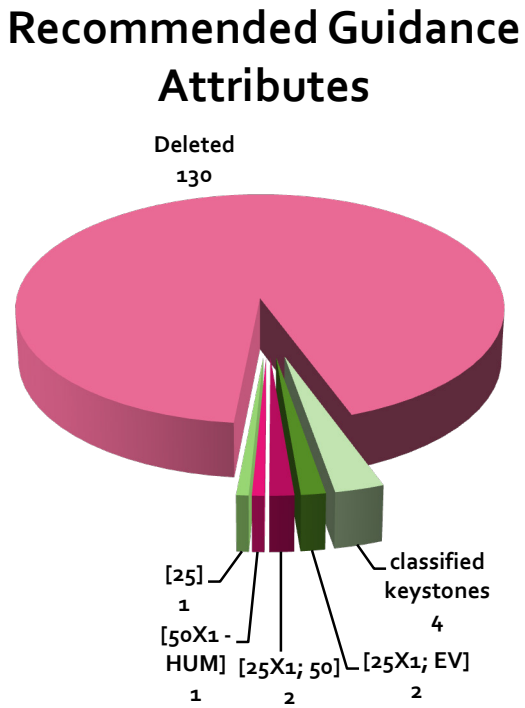
- Delete 27 CI topics in CG-SS-4A and all current CI topics in CG-SS-4 (a total of 9); replace with a CI summary section in CG-SS-4 or its successor.
- Delete most current topics concerning DOE relationships, associations, or agreements with other IC agencies, foreign nationals, or foreign governments because they are not specific enough (will be addressed by CI original classification determinations for each specific relationship, association, or agreement).
- Delete all topics already covered by safeguards and security or other approved DOE guidance.
- Delete all topics that only classify based on other agency guidance, an agreement with a foreign country (i.e., FGI), or source documents.
- Delete most current topics for polygraphs. Modify topic for polygraph equipment for consistency with the Exploitable Design Information keystone. Most other polygraph related information (reason, answers to questions, indications of deception, etc.) is captured by other keystone based topics.

- Delete all current CI-cyber topics as they are dependent on other agency classification or are not specific enough for DC use.
- Retain the overall CI budget classification topic with declassification instruction for referral to DNI with the DOE equity declassified at 25 years.
- Retain five topics based on one or more of the classified keystones.
- Retain a topic for classification of information relating to activities of FIS or indications of targeting or collection under the CI Identification keystone, the DOE equity exempt under 25X1.
- Retain a topic for classification of administrative investigations, preliminary inquiries or incidents of CI concern under the CI Identification keystone, the DOE equity exempt under 25X1.
- Classify all information from a contact report or CI debriefing and exempt from automatic declassification at 25 years under 25X1;50 using the CI Identification keystone to prevent adversary identification of those with specific indications of FIS activities by compilation of all contact reports or debriefings that do not contain such information, or indicate when FIS activities have not been detected.
- Retain topics for classification of identification of other IC agency human sources under the Source Identification keystone and exempt from automatic declassification with 50X1-HUM.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 12 - Enrichment

Current Policy

Classification guidance for the separation and enrichment of plutonium and uranium isotopes is addressed in several Department of Energy (DOE) guidance documents. The majority of information contained in the classification guidance is Restricted Data (RD) under the Atomic Energy Act of 1958, as amended, as the information involves the various methods and technologies to separate the isotopes of uranium and plutonium. However, there are security related topics in the guides that are identified as NSI.

Background

The current guidance is contained in five guides: the *Classification Guide for Isotope Separation by the Gas Centrifuge Process* (CG-IGC-1), the *Joint NRC/DOE Classification Guide for Uranium Isotope Separation by the Gaseous Diffusion Process* (CG-PGD-5), the *DOE Classification Guide for the Plasma Separation Process* (CG-PSP-1), the *Classification Guide for the Separation of Plutonium Isotopes by the AVLIS Method* (CG-SIS-1), and the *Classification and UCNI Guide for Uranium Isotopes Separation by the Atomic Vapor Laser Isotope Separation Process* (CG-UAV-2) . Together, these guides contain 52 National Security Information (NSI) topics: two topics, exempt from automatic declassification at 25 with an event driven declassification; 50 topics that point to other guidance.

Analysis

Analysis revealed the following:

- CG-PGD-5 – Contains thirty-seven topics that point to topics in either the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4) or Nuclear Regulatory Commission (NRC) guidance. Derivative classifiers at United States Enrichment Corporation (USEC) indicated they use the topics in CG-PGD-5, rather than in CG-SS-4, at the direction of the Nuclear Regulatory Commission (NRC). The NRC has now determined no adverse impact would result from removing these topics from CG-PGD-5, and USEC was approved to use CG-SS-4 for the classification of security related gaseous diffusion information. The NRC has agreed these topics can be removed from CG-PGD-5 and that it no longer needs to be a joint guide.
- CG-IGC-1 – Contains two NSI topics; one points to a topic in CG-SS-4, and one topic classifies the details of "cover/disassociated procurements" as Secret NSI, regardless of the material or equipment involved. It was determined that the keystone for this topic was the general methodology behind cover/disassociated procurements. To clarify the topic, it was decided to divide the topic into two subtopics; one to address the general methodology used (which should be declassified, as it did not meet the requirements of Executive Order (EO) 13526, Section 1.2), and a second subtopic to address the details of a particular cover operation, which would remain classified appropriately, per EO 13526, as Secret. Because the topic addressing the general methodology of cover/disassociated

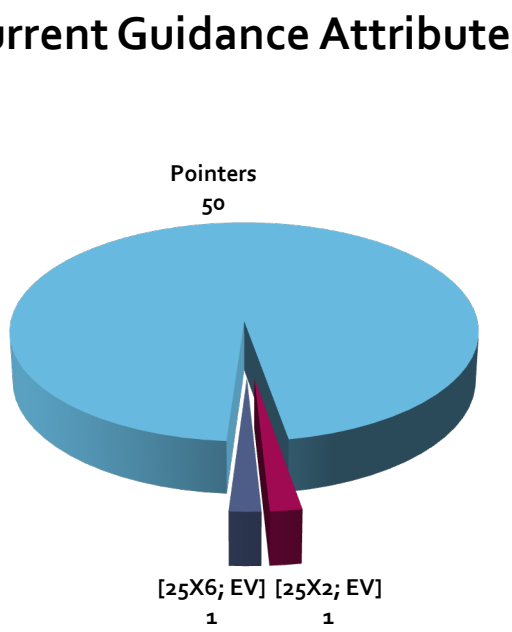
procurements was recommended to be declassified, the definition of "cover operation" is recommended to be unclassified.

- CG-PSP-1 – Contains nine topics; One topic points to a topic in CG-SS-4; eight topics point to one topic in CG-IGC-1
- CG-UAV-1 – Contains three topics; two topics in CG-UAV-2 point to other topics in that guide; one topic points to a topic in CG-SS-4
- CG-SIS-1 – Contains one topic addressing an equity belonging to another agency. The agency confirmed that the classification was correct and that no change was warranted at this time.

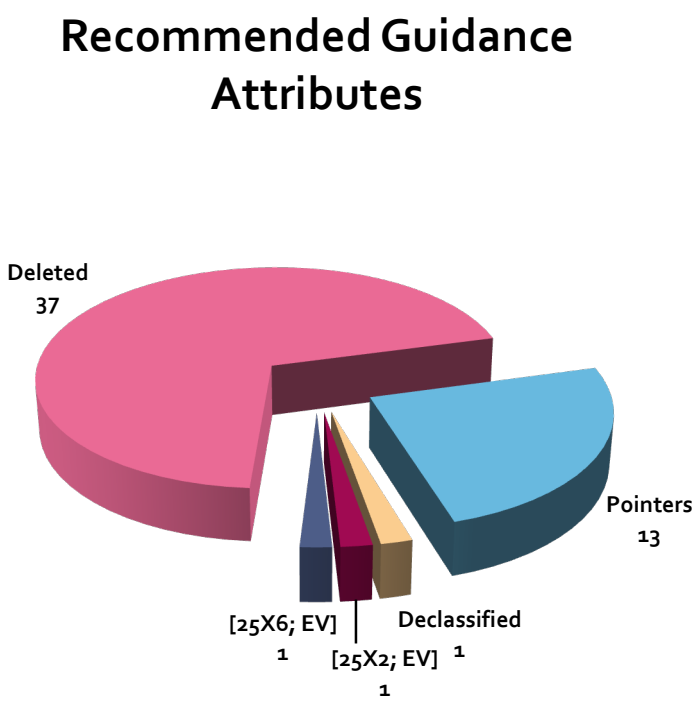
Recommendations

- Delete all 37 safeguards and security related topics from CG-PGD-5 and re-issue the guide as a DOE guide.
- Restructure the single unique topic in CG-IGC-1 into two subtopics, so that the general methodology behind cover/disassociated procurements, along with the definition of a cover/disassociated operation, be declassified; and the details of a particular cover/disassociated operation remain classified at the Secret level. In addition, a caution to warn of RD associations should be added to the Secret subtopic.
- Two topics, exempt from automatic declassification at 25 years with an event driven declassification, thirteen topics will point to other guidance, and 37 redundant topics will be deleted.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 13 - Environmental Sampling

Current Policy

Classification guidance for the Environmental Sampling program addresses information regarding the verification process for compliance with the Limited Test Ban Treaty of 1963, the Threshold Test Ban Treaty of 1974, and the Peaceful Nuclear Explosion Treat of 1976 by detecting possible nuclear explosions. The Air Force Technical Applications Center (AFTAC) is the office responsible for accomplishing this mission.

Background

The current guidance is contained in the *Classification Guide for Environmental Sampling* (CG-ES-1), and the *Supplement to the Classification Guide for Environmental Sampling* (CG-ES-1A). These guides contain 90 National Security Information topics. Additional information on the topics is found in the classified annex to this report.

Analysis

The majority of topics in these two guides point to topics in AFTAC classification guides, and are correctly identified as AFTAC equities. AFTAC provided their guide citation and basis link information for these topics. When AFTAC completes their Fundamental Classification Guidance Review (FCGR) activities, we will implement any changes or updates to these topics accordingly.

Six of the topics were identified as protecting Department of Energy (DOE) information, because the research and development being done to support and enhance the AFTAC environmental sampling programs was conducted and funded by the DOE/National Nuclear Security Administration. Therefore, these six topics are joint equities between DOE and AFTAC.

The only keystone identified is information dealing with foreign relations of the U.S. Government.

Recommendations

- Because six topics are joint equities, change the declassification instructions for these topics to 25X6; 50. This would reflect the declassification instructions only for the DOE portion of the information. Add a caution to these topics specifically stating that the information protected by these topics is a joint equity and, as such, must be referred to the Air Force for declassification of their equities.
- Reword several topics in order to provide a better description of the information being protected.
- When AFTAC completes their FCGR activities, update the two guides accordingly for the joint equities.

For more detail regarding these recommendations, see the classified annex to this report.

Working Group 14 – Material Protection, Control and Accountability

Current Policy

Classification guidance for the MPC&A program addresses program information, location/asset description, threat description, risk assessment, and protection systems. The MPC&A program follows a systematic methodology in assisting foreign governments in nuclear safety upgrades.

Background

The current guidance is contained in the *Classification Guide for MPC&A Information* (CG-MPCA-1) and the *Annex to the Classification Guide for MPC&A Information* (MPCA-1A). These guides contain 115 National Security Information (NSI) topics.

Analysis

Three keystones related to foreign relations were identified.

Topics in both guides protect information provided to NA-25 during official government correspondence. Currently this information ranges from C/FGI-MOD to SNSI. The range of classification is based on an assessment of the damage done by releasing this information. Currently, one topic series in both guides contains topics classified as C/FGI-MOD, CNSI, and SNSI. During analysis, it was determined that this information was always determined to be either C/FGI-MOD or SNSI. Therefore, the CNSI topic in the series will be deleted from both guides.

Because the information classified in the MPC&A program is derived from treaties or agreements with foreign governments, these topics could also be exempted from automatic declassification under 25X9.

Recommendations

Because information in topic series discussed above is always determined to be either C/FGI-MOD or SNSI, delete the CNSI topic in this topic series from both CG-MPCA-1 and CG-MPCA-1A.

For additional details, refer to the classified annex of this report.

Working Group 15 - Nuclear Smuggling

Current Policy

Classification guidance for Nuclear Smuggling applies to information regarding Department of Energy (DOE), National Nuclear Security Administration (NNSA), and Department of Homeland Security (DHS) Customs and Border Protection (CBP) activities and detection systems related to nuclear smuggling.

Background

The current guidance is contained in *Joint CBP/DOE Classification Guide for Nuclear Smuggling Information* (CG-SMG-2). This classification guide was developed as a joint guide with CBP because, at the time of development, the DHS did not have the infrastructure in place to develop, produce, and distribute the guide. The DOE does not have a nuclear smuggling detection program, although several National Laboratories conduct activities in support of DHS.

Analysis

CG-SMG-2 contains 31 NSI topics. All 31 topics either point to other DOE or DHS guidance. All topics were forwarded to the DHS classification office and the NNSA Office of Emergency Response (NA-42) for review. After review, it was confirmed that all DOE information being protected is adequately identified in other DOE guidance such as CG-RDD-1*, Joint DOE/DHS/NRC Classification Guide for Radiological Dispersal Devices and Radiation Exposure Devices*, CG- RER-1, *DOE Classification and UCNI Guide for Radiological Emergency Response*, and others. There are no original DOE keystones identified in CG-SMG-2. DHS has agreed to convert this guide to a DHS classification guide.

Recommendations

DOE assist DHS to develop a DHS only classification guide for activities and detection systems related to nuclear smuggling. Upon completion of DHS guide, DOE will cancel CG-SMG-2.

Working Group 16 – Nuclear Materials

Current Policy

Classification guidance concerning nuclear materials applies to the various nuclear materials that have been produced for nuclear weapon purposes. The majority of classification information created that concerns materials production meets the requirements of Restricted Data (RD), per the Atomic Energy Act of 1958, as amended.

Background

The current guidance is contained in the *DOE Classification Guide for Nuclear Materials Production* (CG-NMP-2). There are 16 National Security Information (NSI) topics. These topics consist of:

- Two topics exempt from automatic declassification at 25 years, with an event driven declassification.
- Fourteen topics that point to other guidance.

Analysis

No Department of Energy (DOE) keystones were identified during the analysis.

- The majority of the pointer topics refer the derivative classifier to safeguards and security guidance concerning the shipment or transfer of quantities of materials. Some of this information exists in program specific guidance.
- One topic was determined to be a Department of Defense (DoD) equity, which was confirmed by the Defense Threat Reduction Agency.
- Two topics contain the phrase "RD/may be NSI" as a part of the classification determination. These topics point to information in the *Joint DOE/DoD Topical Classification Guide for Weapon Production and Military Use (TCG-WPMU-2)*, which was reviewed by Working Group 25, WPMU, who determined that this information would not be NSI.

Recommendations

- Revise the topic regarding the DoD equity to include the instruction "Refer to DoD," as the responsible agency.
- Revise the two topics pointing to TCG-WPMU-2 by removing "may be NSI" from the determination of these topics.

Working Group 17 - Materials Disposition

Current Policy

The Fissile Materials Disposition Program is responsible for the handling of weapon usable fissile materials that are surplus to the national security needs of the United States (U.S.). It is the policy of the U.S. Government to protect sensitive nuclear weapon technology and production information that may be revealed by the materials being declared surplus. To that end, the Department of Energy (DOE) generated classification guidance provided in the *DOE Classification Guide for the Fissile Materials Disposition Program* (CG-MD-2), and subsequently in the *Classification Guidance for International Atomic Energy Inspections at DOE Facilities* (TNP-8). TNP-8 was written to provide additional classification guidance for activities involving International Atomic Energy Agency (IAEA) inspections at DOE facilities.

Background

The guidance in CG-MD-2 contains 8 National Security Information (NSI) topics. The topics cover shipment, quantity/location, quantities identified for monitoring by the IAEA, security, and deep borehole disposition of surplus Special Nuclear Material (SNM). These topics consist of:

- One that requires declassification at 25 years.
- Three that are exempt from automatic declassification at 25 years.
- Four that point to other classification guidance.

TNP-8 contains two NSI topics. The topics cover data transmitted by safeguards sensors and information conveyed by analytical samples of SNM. Both of these topics point to other classification guidance.

Analysis

Only one keystone was identified that required protection - SNM safeguards of plutonium placed in deep boreholes.

The working group reviewed several pointer topics with a note pointing back to *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), the guide containing the root topics for the type of information described. The working group determined that these pointer topics are CNSI for unreconciled inventories and Restricted Data when weapon information is revealed. Notes will be added to these topics to aid the user in determining the appropriate classification.

One topic covers the classification of enriched uranium not allocated to weapons programs at the Y-12 site. The topic has an Unclassified (U)/CNSI classification and refers the user to the CG-SS-4 for further information. The working group determined that a note referring users to the Y-12 classification office for help determining when the information was classified would be beneficial. Additionally, a note directing the user to the Nuclear Material Control and Accountability (MC&A) section of CG-SS-4 would improve the quality of guidance.

IAEA safeguards for HEU are covered by a series of topics in CG-MD-2. The guidance classifies exact quantities of enriched uranium under IAEA safeguards. This information was classified based on the premise that the information indicated target attractiveness to an adversary. This concept was removed from other guidance in September 2000 with the release of CG-SS-4. This information should only be classified based on whether the inventory is reconciled and audited, as well as any programmatic issues; therefore, a pointer to CG-SS-4 MC&A topics concerning reconciliation of inventories is appropriate. (See Working Group 9, MC&A for additional information on this subject area.) The working group also determined the need to address plutonium in the IAEA section in order to enable use for all envisioned scenarios across the complex.

The final topic reviewed concerns the burial of surplus plutonium that does not meet the spent fuel standard in deep boreholes. The spent fuel standard is a concept developed in the early 1990s to dispose of surplus weapons grade plutonium. The topic has a U/CNSI classification but does not indicate when either level applies. The original version of the guide contained a note that indicated the information is U when declassified and released by DOE. This note was removed in a subsequent revision to CG-MD-1 without any explanation in the guide development file. Since DOE can make the decision to declassify the information if desired, the note and U/CNSI [25] classification is unnecessary. The working group determined that the information warranted classification for 25 years. It is recommended to change the topic to CNSI [25].

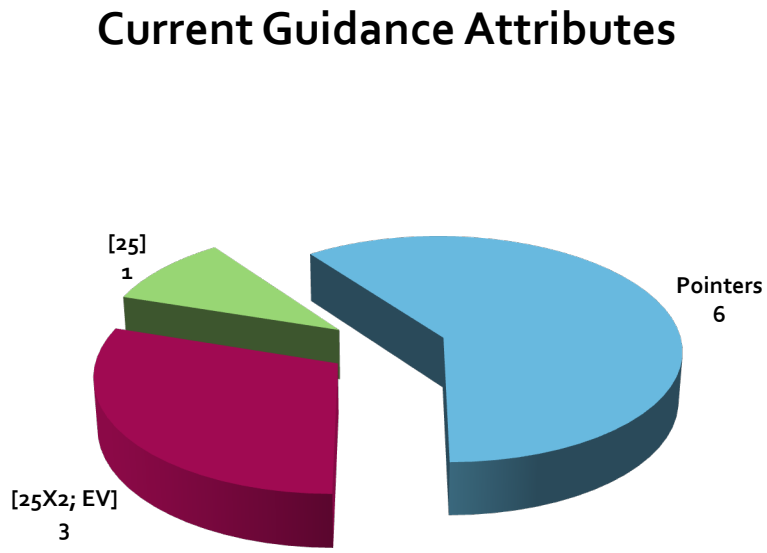
All three of the 25X2; EV topics reviewed were found to be either a pointer, an EV topic not requiring a 25-year exemption, or no longer considered to be classified information. In one of these cases, the declassification event for the activity has occurred, so the information is now unclassified. In the other, the information was declassified when CG-SS-4 was approved in September 2000, making the topic inconsistent with the root guidance.

Recommendations

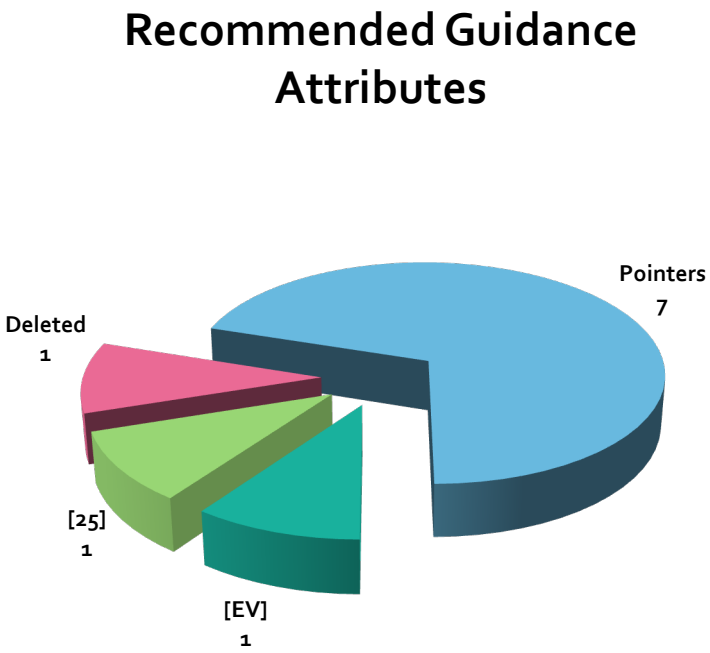
The guidance should be rewritten to reflect the recommendations of the working group:

- Revise one topic to indicate that the related information is unclassified due to declassification event occurring.
- Delete one 25X2 topic.
- Change one topic from 25X2; EV to EV.
- Convert one topic to a pointer.
- Cancel TNP-8 by incorporating two pointer topics into CG-MD-2.
- Revise guidance related to IAEA safeguards activities to cover plutonium as well as highly enriched uranium.
- Improve four pointer topics and one keystone topic by clarifying notes to aid derivative classifiers in applying the topics correctly.
- Add a definition for the spent fuel standard.
- Additionally, to aid the user, a note describing when plutonium meets the spent fuel standard is added to a topic.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 18 - Power Systems

Current Policy

As part of its responsibilities under the Atomic Energy Act of 1954, as amended, the Department of Energy (DOE) designs and/or builds radioisotope and nuclear reactor power systems for various space exploration and national security applications. At various times over the history of the department and its precursor organizations, interagency programs have operated to design and build nuclear reactors and radioisotope power systems for terrestrial and space military applications. These programs produced extensive information on materials and design engineering solutions to the challenging problems encountered in these applications. It is the policy of the U.S. Government to protect this information when it significantly assists the efforts of others to build similar systems.

Four joint guides provide guidance on which aspects of these technologies are classified. They are:

- The *Joint DOE/DoD/NASA Classification Guide for Radioisotope Power Systems* (CG-RP-1).
- The *DOE/DoD/NASA Classification Guide for Space Reactor Power Systems* (CG-SRPS-1).
- The *Joint DOE-NASA Classification Guide for Civilian Space Nuclear Reactors to Support NASA Project Prometheus Missions* (CG-SNR-1).
- The *Joint DOE/DoD Classification Guide for the Army Nuclear Power Program (*CG-RAR-6).

Background

CG-RP-1 contains 13 National Security Information (NSI) topics. The topics cover programmatic, mission, design, and safety information for radioisotope based power systems. These topics consist of:

- Two that require declassification at 25 years.
- One that is declassified after an event occurs.
- Ten that refer to other classification guidance.

CG-SRPS-1 contains 44 NSI topics. The topics cover programmatic, research and development (R&D), procurement, specifications, fabrication, testing, design, military requirements, and security information for space reactor power systems. These topics consist of:

- Twenty-eight that require declassification at 25 years.
- Sixteen that refer to other classification guidance.

CG-SNR-1 contains 23 NSI topics. The topics cover programmatic, R&D, design, transportation, safety and security information for space reactor power systems for the Prometheus Missions (no missions occurred; the program cancelled). These topics consist of:

- Nine topics exempt from automatic declassification at 25 years because the release would reveal information that would cause serious harm to relations between the U.S. and a FG, or to ongoing diplomatic activities of the U.S.; or violate a statute, treaty, or international agreement that does not permit automatic declassification at 25 years (25X6, 9).
- Fourteen that refer to other classification guidance.

CG-RAR-6 contains 1 NSI topic. This topic, which covers the development of new army nuclear reactors, refers to other classification guidance.

Analysis

Eight keystones were identified that require protection:

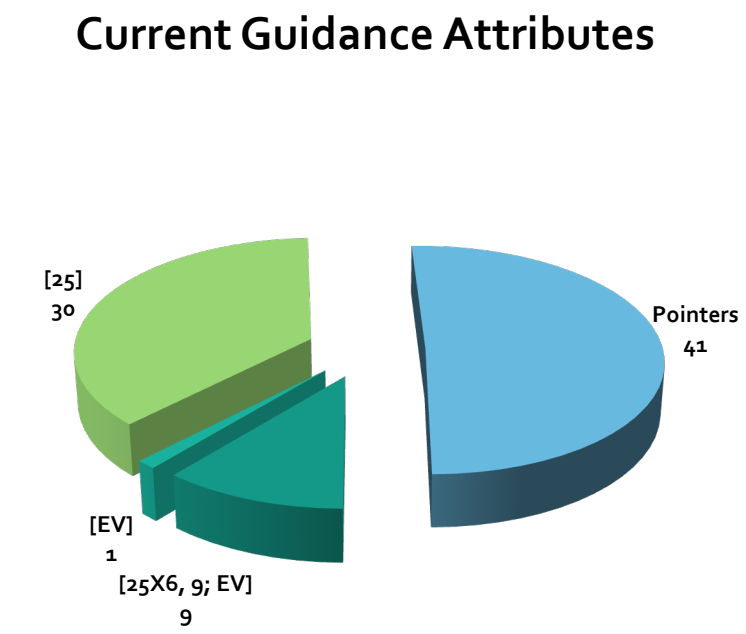
- Space reactor design
- Space reactor material
- Space mission data
- Hardening
- Special Nuclear Material (SNM) - Vulnerable location
- SNM - Safeguards
- SNM - Allocation
- SNM – Recovery

In CG-SRPS-1 there are 30 topics that cover space reactor power system military requirements and applications. These topics originate in some uses for space reactors envisioned as part of the Strategic Defense Initiative of the 1980s. The superseding agency, the Missile Defense Agency, determined that this is their equity and no longer requires protection and should be declassified. The working group determined that the durations of classification were appropriate in all cases. No changes are recommended for the guidance in CG-SNR-1 or CG-RAR-6.

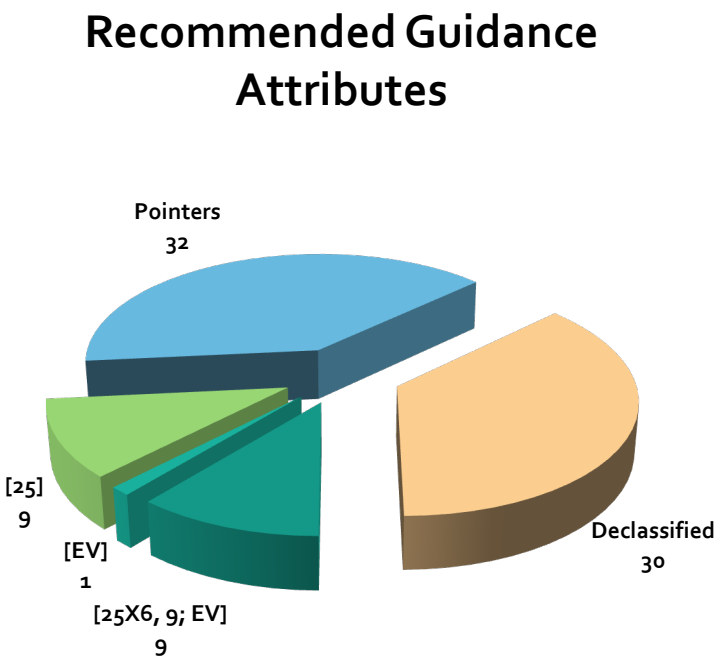
Recommendations

- Merge CG-RP-1 and CG-SRPS-1 into one modernized guide to address current projects while retaining topics applicable to legacy programs.
- Deletion of 30 topics related to the Strategic Defense Initiative which relate to information that has been declassified by the Department of Defense.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 19 - Russian Materials

Current Policy

The Highly Enriched Uranium (HEU) Transparency Program is responsible for the purchase of low enriched uranium derived from HEU removed from dismantled Russian Federation (R.F.) nuclear weapons. The program is governed by the U.S.-R.F. Purchase Agreement, signed in February 1993. R.F. information, as well as U.S. information related to this program is classified in accordance with the guidance provided in the *Classification Guide for Highly Enriched Uranium Transparency Program* (CG-TP-1).

Additionally, the U.S. periodically purchases plutonium-238 from the R.F. for use in radioisotope based power sources used in civilian space exploration missions. Various details regarding the classification of transportation information regarding these purchases are classified in accordance with the guidance provided in *Guidance for the Shipment and Receipt of Plutonium-238 from the Russian Federation* (TNP-30).

Background

The guidance in CG-TP-1 contains 49 National Security Information (NSI) topics. The topics cover programmatic, facility, equipment, process, transportation, and transparency assurance information generated by the HEU Transparency Program. These topics consist of:

- Forty-two that are exempt from automatic declassification at 25 years.
- Seven that point to other classification guidance.

The guidance in TNP-30 contains three NSI topics. The topics cover transportation information related to the purchase of plutonium-238 from the R.F. These topics consist of:

- Two topics that require declassification at 25 years.
- One topic points to other classification guidance.

Analysis

In performing this review, the working group identified six keystones that required protection:

- Negotiation positions
- HEU agreement information
- Arms control
- Special Nuclear Material (SNM) – Transport
- Foreign facility – vulnerability
- Material verification

For the 25X6 topics, 25 topics should be changed to 25X9 because the information is related to information provided to the program by the R. F. under the agreement. The remaining 25X6

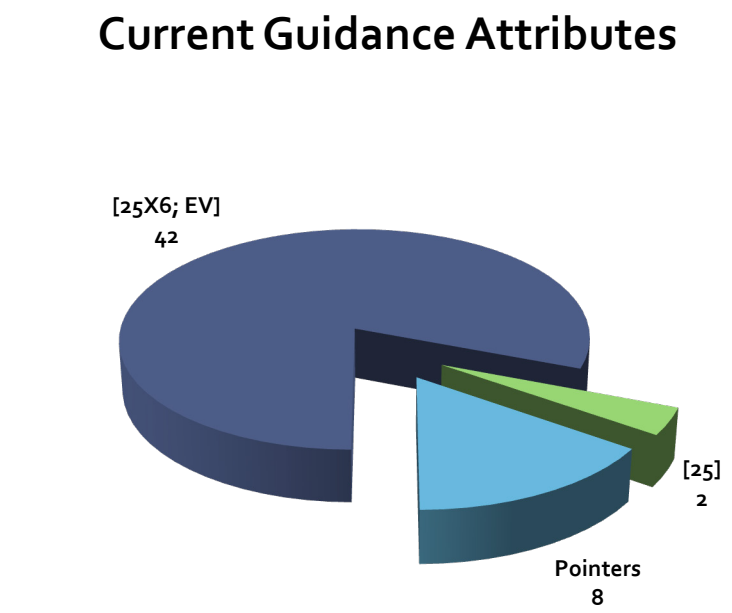
topics cover information that would affect relations with the R.F. but are not specifically addressed or covered by the agreement, so 25X6 is appropriate.

Four topics have a reference added to the declassification instructions to refer to the Department of State (DOS) to determine when the information would no longer harm foreign relations with the R.F. Ten topics should be rewritten for clarity. Finally, one pointer topic requires correction by inclusion of the 25X6 exemption listed with the parent topic in the *DOE Classification Guide for Nonproliferation of Weapons Information* (CG-NP-3).
The durations of classification are appropriate. No changes are recommended for the guidance in TNP-30.

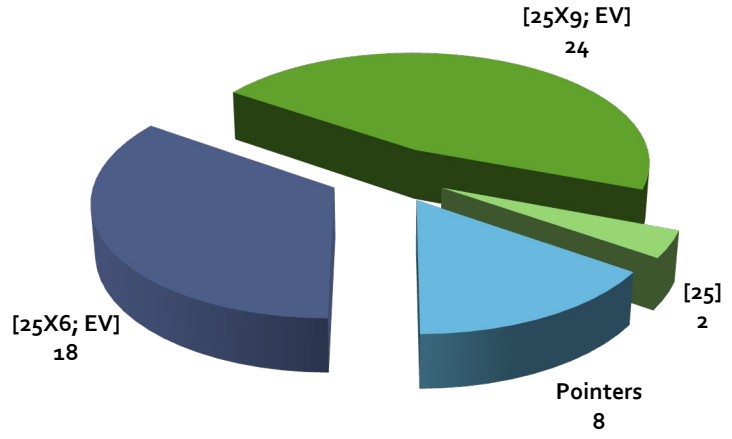
Recommendation

- Revise the exemption criteria for 25 topics in CG-TP-1 from 25X6 to 25X9.
- Revise the declassification instructions for four topics to refer the information to DOS.
- Reword ten topics for clarity and to make application of topics easier.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 20 - International Safeguards

Current Policy

The International Safeguards Working Group examined classification guidance used by Department of Energy (DOE)/National Nuclear Security Administration (NNSA) programs designed to acquire/secure Special Nuclear Material (SNM) owned by foreign nations that is considered at risk for proliferation. It is in the interest of the U.S. Government to classify information about various aspects of the projects in order to protect foreign relations, operational security, and national security. To that end, DOE generated classification guidance contained in the *Classification Guide for a Material Protection Project* (CG-MPP-2); *Classification Guidance for Operation Sapphire* (TNP-3); *Classification Guidance for a Material Protection Program* (TNP-11); and *Classification Guide for Non-U.S. Reactor Conversion Studies* (CG-RC-2).

Background

The National Security Information (NSI) topics in CG-MPP-2, TNP-3, and TNP-11 cover programmatic, foreign relations, facility, packaging, and transportation information associated with Project Maximus, Project McCall, Sapphire, Olympus, Auburn Endeavor, and Partnership. The guidance in CG-MPP-2 contains 23 NSI topics. Of these topics:

- Two are exempt from automatic declassification.
- Six require declassification at 25 years.
- Fifteen that refer to other classification guidance.

The guidance in TNP-3 contains 13 NSI topics. These topics consist of:

- Nine that are exempt from automatic declassification.
- Four that point to other classification guidance.

The guidance in TNP-11 contains 21 NSI topics. All 21 topics are exempt from automatic declassification.

The guidance in CG-RC-2 contains seven NSI topics. The topics cover information related to projects to exchange foreign research reactor highly enriched uranium fuel rods for low enriched uranium fuel rods. All seven topics are exempt from automatic declassification.

Analysis

Four keystones were identified that require protection:

- Foreign relations
- SNM – Safeguards
- SNM – Packaging
- SNM – Transport

In CG-MPP-2, one topic regarding technical and repackaging difficulties should be declassified, since Project Maximus is complete and the SNM is secure. Three topics cover compensation and forms of assistance provided to the Government of Iraq in exchange for the SNM. All three are U/CNSI topics with no indicators of what makes the information CNSI. This information, an equity of the Department of State, should be referred to them for classification.

TNP-3 also has one topic related to compensation provided in exchange for SNM which should be revised to refer the information to the Department of State (DOS).

TNP-11 has one topic that should be split into two topics in order to properly classify the U.S. facility portion of the topic with a 25-year duration, in line with the parent topic for the information in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4).

CG-RC-2 has guidance that is not in alignment with how the program office conducts reactor conversion projects. A complete restructuring and alignment of the guidance with current programmatic needs is recommended.

Recommendations

The guidance should be revised to:

- Merge CG-MPP-2, TNP-3, and TNP-11 into a single guide with common topics consolidated and Executive Order 12958 based topics updated. This will enable cancellation of the two bulletins and reduce guide maintenance and potential inconsistency.
- Declassify one topic related to packaging issues in CG-MPP-2.
- Revise four topics to refer the user to DOS for a classification determination.
- Rewrite CG-RC-2 to reflect how the reactor conversion projects are managed and operated.

Working Group 21 – Radiological Dispersal Devices

Current Policy

The Department of Energy (DOE) maintains classification guidance related to radiological dispersal devices (RDDs) and radiation exposures devices (REDs). RDDs and REDs are considered weapons of mass destruction (WMDs) which present a significant and continuing threat to the national security of the United States. The guidance addresses the properties and design of these devices, their dispersal patterns, effects, and recovery actions. This guidance is maintained by DOE and implemented jointly by DOE, the Department of Homeland Security (DHS), and the Nuclear Regulatory Commission (NRC).

Background

The *Joint DOE/DHS/NRC Classification Guide for Radiological Dispersal Devices and Radiation Exposure Devices* (CG-RDD-1) contains 45 topics addressing National Security Information (NSI); 6 topics point to other classification guidance topics; and 39 topics (35 Secret and 4 Confidential) are unique to the RDD/RED subject area and required analysis by the working group.

When CG-RDD-1 was approved in September 2009, the signatories intended that a thorough review and rewrite of the guide would be conducted after the guide had been used for a year and feedback was received from the field. The Fundamental Classification Guidance Review is being conducted concurrently with this rewrite of the guide.

Analysis

The 39 unique topics in CG-RDD-1 are exempt from automatic declassification at 25 years as the release of which would reveal information that would assist in the development or use of WMDs, and have event driven declassifications. The declassification event throughout the guide is identified as "when the technology is no longer applicable to use in RDDs or REDs, or official disclosure of the technology has been made."

The 39 unique RDD/RED topics protect three keystones of information:

- Identification, design, or optimization of unique technologies for radiological dispersal or radiation exposure.
- Non-explosive RDD techniques.
- Provocative information which might encourage an RDD/RED attack.

The rewrite of CG-RDD-1 is almost complete. Six topics have been rewritten to include subtopics with references to specific classification levels, thereby reducing the instances where a derivative classifier had to choose a classification from an Unclassified (U)-Secret (S) NSI range with minimal guidance. The working group agreed to focus on the attributes of the specific radioactive material in determining classification. Use in an RDD of radioactive material that was in a form found in common usage by industry, commerce, or medicine would be

unclassified. Examples include cesium chloride used in self-contained irradiators and americium oxide used as well logging sources.

The working group recognized that the consequences of an RDD event were significantly greater than those of an RED event. Consequently, the group concluded RDD information would be classified at the S level and similar information for REDs would be classified at the Confidential (C) level.

The working group determined that all topics protecting the three keystones identified above should be exempt from automatic declassification at 50 years and cite the WMD reason for classification in the Executive Order 13526, section 3.3(h)(1)(B). Therefore, justification for these topics has been sent to the Interagency Security Classification Appeals Panel, via the Information Security Oversight Office, for approval.

Twenty of the topics were retained as written; however, all declassification instructions were revised to 50X2 as described above.

Recommendations

- Revise all 39 topics to require exemption from automatic declassification at 50 years.
- Classify the use of specified radioactive materials in an RDD or RED based on whether the material is in a form as commonly found in medical, industrial, or commercial uses (U) or if the material has been modified from the common form (SNSI).
- Limit the classification of REDs to CNSI.

Working Group 22 – Weapon Outputs

Current Policy

The majority of information related to nuclear weapon outputs is Restricted Data, with the exception of intelligence-related information which is National Security Information (NSI).

Background

The *Joint DOE/DoD Classification Guide for Weapon Outputs* (TCG-WO-1) is the classification guide in this subject area that contains NSI topics. The guide contains two NSI topics:

- One topic refers to the source documents from which the information on the outputs of non-U.S. weapons originated (in order to determine classification level, category and declassification instructions).
- One topic is for intelligence evaluations which are classified at either the Secret or Top Secret level.

Analysis

The first topic refers to the source documents in order to determine classification level, category, and declassification instructions.

The second topic is a Director of Central Intelligence (DCI) equity. The topics should refer the derivative classifier to the DCI organization for declassification instructions.

Recommendations

- Retain the first NSI topic as is.
- Revise the second NSI topic to delete the declassification schedule and refer the derivative classifier to the DCI for declassification instructions.

Working Group 23 - Malevolent Dispersal/Threat Messages

Current Policy

The Department of Energy (DOE) maintains guidance to classify information involving (1) the malevolent dispersal of radioactive materials and (2) threat messages received from a perpetrator. Because of involvement by multiple government agencies in planning and executing coordinated responses to such events, including performance of training exercises, DOE works with agencies such as the Department of Homeland Security and the Federal Bureau of Investigation to develop joint classification guidance.

Background

The guidance reviewed by this working group is located in two sections of the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4). Guidance concerning these two subject areas is also contained in other classification guides.

Malevolent Dispersal – The malevolent dispersal of radioactive material from a device constructed by an adversary or perpetrator is addressed in the *Joint DOE/DHS/NRC Classification Guide for Radiological Dispersal Devices and Radiological Exposure Devices* (CG-RDD-1). This section of CG-SS-4 contains six NSI topics. Four of the topics refer the derivative classifier to other topics in CG-SS-4, and one points to the *DOE Classification and UCNI Guide for Radiological Emergency Response* (CG-RER-1). The remaining topic is unique and addresses specific dispersal test and analysis information.

Threat Messages - Nuclear threat messages are also addressed in CG-RER-1 and the *DHS/DOE Classification and UCNI Guide for Nuclear/Radiological Incident Emergency Response and Consequence Management* (CG-NRI-1).

All seven topics refer to, or are based on, other portions of CG-SS-4 or CG-RER-1.

Analysis

Malevolent Dispersal – Some vulnerability topics inadequately address certain radiological dispersal and sabotage scenarios. The vulnerability-related topics were assessed to resolve this shortcoming. The topic which refers to CG-RER-1 deals with radiological dispersal devices (RDD) and should refer to CG-RDD-1. A more effective means for this reference would be via a general note placed at the beginning of the topic section. There is one unique topic with a specified duration of 25 years that is appropriate. However, it was recognized that information classified by this topic could possibly contain Safeguards Information (SGI) under the purview of the Nuclear Regulatory Commission (NRC) when automatically declassified.

Keystone – for the unique topic, the keystone being protected is the results of dispersal tests or experiments, and subsequent analysis.

Three topics pointing to other guidance contain some classification/declassification instructions that are extraneous to the pointing function.

Threat Messages - Seven topics pointing to, or based on, other guidance are appropriate.

Recommendations

Malevolent Dispersal

- Add a general note at the beginning of this topic section to restrict its applicability solely to dispersal of radioactive materials in storage or in process at or in transit to or from DOE facilities. This separates its applicability from the device dispersals addressed more broadly by CG-RDD-1.
- Delete the topic dealing with RDDs.
- Add a note to one topic informing the user of a possible residual NRC SGI equity upon declassification of the information.
- Remove unnecessary classification/declassification instructions from the three topics which point the user to other guidance.

Threat Messages:

- Retain the seven topics that refer to, or are based on, other relevant guidance.

Working Group 24 - Radiological Emergency Response (RER)

Current Policy

The Department of Energy (DOE) maintains guidance to appropriately classify information involving DOE's actions in response to radiological emergencies. A significant portion of Radiological Emergency Response (RER) activity is an interagency effort, including the DOE/National Nuclear Security Administration (NNSA) RER assets [that function as the Nuclear Emergency Support Team], operating under the direction of a Lead Federal Agency (LFA) that has been designated for the specific response mission (and may change depending on the nature of the emergency). *DOE Classification and UCNI Guide for Radiological Emergency Response* (CG-RER-1) addresses the RER issues from a DOE standpoint – RER personnel and equipment; general mission/training operations; threat device information; and details of specific phases of RER operations, including Crisis Response and Consequence Management. It also contains a significant topic section dealing with the assessment/handling of nuclear threat messages received from a perpetrator.

In addition, the *DHS/DOE Classification and UCNI Guide for Nuclear/Radiological Incident Emergency Response and Consequence Management* (CG-NRI-1) covers essentially the same material contained in CG-RER-1, subject to the limitation that the guide is Official Use Only, versus Secret Restricted Data. It is a guide issued jointly by DOE and the Department of Homeland Security (DHS).

Background

CG-RER-1 contains 153 topics addressing classified National Security Information (NSI). Of these:

- Nineteen topics point the user to other DOE guidance – usually the *Joint DOE/DHS/NRC Classification Guide for Radiological Dispersal Devices and Radiation Exposure Devices* (CG-RDD-1).
- Twelve topics point the user to guidance from another Government agency – usually to the DHS. When CG-RER-1 was originally approved in 2002, DOE was responsible for the Nuclear Assessment Program (NAP) and the assessment of nuclear threat messages. This is now a DHS function, with the NAP managed by the Domestic Nuclear Detection Office.
- Six topics have their basis in other DOE guidance – almost all in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4), or the *Transportation Safeguards System Classification and Unclassified Controlled Nuclear Information Guide* (CG-TSS-3). These topics deal with security for training and actual threat devices.

Of the remaining 116 NSI topics, a significant portion (53) entail a range of classification/control possibilities, with the appropriate determination to be received from the LFA for a specific RER mission or training exercise, via communication from a DOE Senior Energy Official (SEO) or Emergency Response Officer (ERO). CG-RER-1 calls for the publication of supplemental

guidance for each training exercise to formalize classification determinations (to include duration of classification) in advance of the exercise.

CG-NRI-1 contains 88 topics addressing classified NSI; however, all of these topics are either based on other guidance (nearly all from CG-RER-1) or point the user to other guidance.

Analysis

Nine prominent keystones were identified for DOE information addressed by CG-RER-1:

- Eight are categorized as being critical nuclear accident or counterterrorism incident response (NCTIR) capabilities and vulnerabilities, further applied to the specific mission areas of searching for, diagnosing, modeling, and defeating nuclear/radiological threats.
    - NCTIR search capability
    - NCTIR search vulnerability
    - NCTIR diagnostic capability
    - NCTIR diagnostic vulnerability
    - NCTIR modeling capability
    - NCTIR modeling vulnerability
    - NCTIR defeat capability
    - NCTIR defeat vulnerability
- The remaining keystone consists of tactics, techniques, or procedures used in NCTIR operations.
    - NCTIR tactic, technique, or procedure

In CG-RER-1, 76 of the 153 topics designated an event for the duration of classification. In 15 cases, the event descriptions were found to be adequate and the topic was left unchanged. In two additional instances, the event description was rewritten to be sufficiently specific and identifiable. However, for many of the remaining 61 topics, it was found that an adequate event description could not be formulated and an alternate disposition (e.g., declassification or referral to other guidance) was not appropriate. Thus, a total of 41 topics had their duration changed from EV to 50 years.

Five topics were determined to no longer warrant classification beyond 25 years, and exemption codes 25X2 and 25X8 were removed from their classification duration. An additional five topics were determined to no longer warrant classification and were recommended for declassification. Three of these topics deal with the identification of fissile materials contained in specific nuclear threat devices and no longer have a basis for classification as NSI. A fourth topic dealing with NEST response times also no longer has a basis for classification as NSI. The fifth topic deals with NEST personnel and had its wording revised to narrow its applicability to unclassified information.

In validating event descriptions, it was discovered that 13 topics dealing with certain threat device render-safe technology were based on guidance from the Defense Advanced Research Projects Agency, but the guidance had been cancelled. DOE determined there was a need to continue to classify this information since there is a DOE equity. This guidance will be

incorporated into a revision of CG-RER-1 via an original classification decision by the DOE OC OCA.

The original 12 topics which referred the user to other agency guidance were not changed. However, nine other topics related to NAP activities were changed to refer to DHS guidance, because they are not DOE equities.

In current guidance, 48 topics rely on the ERO/SEO for classification/declassification decisions. This is unnecessarily burdensome, and the conditions identified in many of these topics are not specific enough to apply consistently. In attempting to address information that has many unique facets that would or would not make it classified, these topics inadvertently place the ERO/SEO in the position of determining the level of damage caused to national security by the release of the information. In addition, the information frequently falls under the cognizance of additional agencies involved in the interagency response activity.

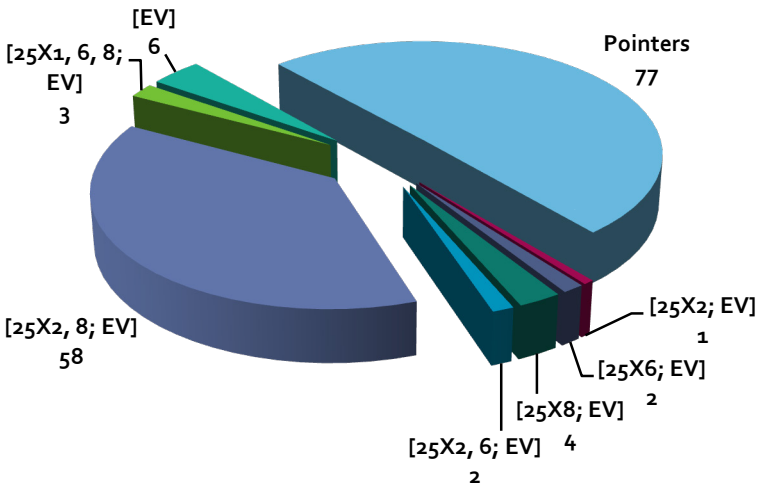
Recommendations

Rather than retaining broad topics, a DOE/NNSA Office of Emergency Operations original classification authority for RER should classify specific information about DOE participation in specific RER activities that meets the requirements for classification (demonstrable damage to national security, etc.); this original classification will then be the basis for DOE derivative classification guidance for that specific information.

Revise the guidance to better reflect current agency roles/responsibilities jointly with the Federal Bureau of Investigation and DHS.

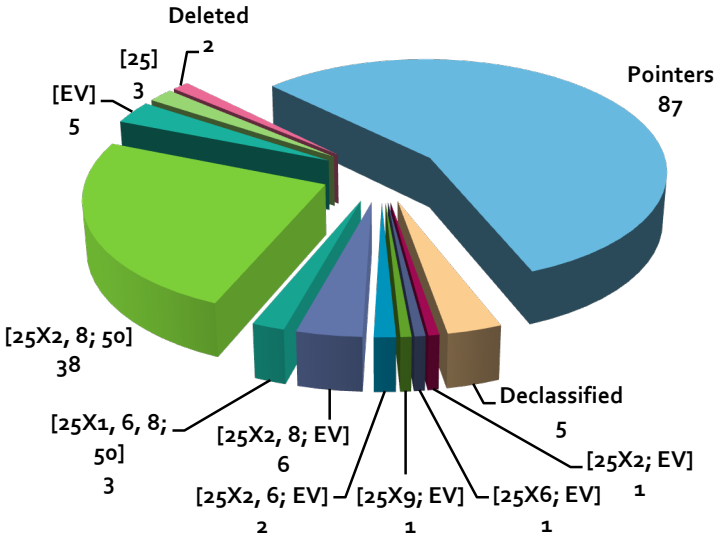
The following chart identifies the declassification events used in the current guidance:

Current Guidance Attributes



The following chart identifies the changes from the current guidance:

Recommended Guidance Attributes



Working Group 25 - Weapon Production and Military Use

Current Policy

National Security Information (NSI) topics covered the areas of nuclear weapon production and use/employment of nuclear weapons, as well as accidents involving nuclear weapons over the past 60 years. The NSI topics in the five guides involve the areas of transportation of nuclear weapons or components and/or safeguards and security of nuclear weapons throughout the complex. The current guidance is inadequate as too much discretion is left to derivative classifiers and derivative declassifiers.

Background

The Weapon Production and Military Use (WPMU) working group examined the NSI topics in the following 5 classification guides:

- *Joint DOE/DoD Topical Classification Guide for Weapon Production and Military Use* (TCG-WPMU-2)
- *Joint DOE/DoD Topical Classification Guide for Detonation Systems* (TCG-DS-2)
- *DOE/DoD Topical Classification Guide for Weapon Initiators* (TCG-WI-2)
- *Joint DOE/DoD Topical Classification Guide for Safing, Arming, Fuzing and Firing* (TCG-SAFF-2)
- *Joint DOE/DoD Topical Classification Guide for Vulnerability and Hardening* (TCG-VH-2)

Analysis

These 5 classification guides contain 27 NSI topics. TCG-WPMU-2 contains 20 topics. Of those:

- Six topics represent Department of Energy (DOE) equities and refer to other topics within the guide or other guides.
- Four topics represent equities shared jointly between DOE and Department of Defense (DoD). All four are exempt from declassification at 25 years with event based declassification instructions. One refers to other appropriate agency-specific guidance and three are situation dependent.
- Ten topics represent equities belonging to DoD and the Department of State (DOS).

TCG-DS-2 contains 4 topics that represent equities shared jointly between DOE and DoD; all four are situation dependent.

TCG-WI-2 contains one topic that refers to a topic in another guide.

TCG-SAFF-2 contains one topic that is exempt from declassification at 25 years and contains event-based declassification instructions.

TCG-VH-2 contains one topic representing an equity belonging to the Intelligence Community.

The Fundamental Classification Guidance Review was being conducted concurrently with the rewrite of TCG-WPMU-2. The ten DoD/DOS joint equity topics in TCG-WPMU-2 were determined to be unnecessary, as they contained the caveat "may be NSI," which was determined to be incorrect. Of the four joint equity topics, one was determined to be redundant to a topic in another guide, one was determined necessary but with an incorrect range of U-TSNSI, and other two topics were determined necessary but required a change from event-based declassification instructions to a more appropriate classification duration of 25 years.

The four topics in TCG-DS-2 were determined necessary to retain in the guide, to provide appropriate instruction to the derivative classifier for when to classify as NSI and when to classify as Restricted Data. The event-based declassification instructions were determined to be correct.

The keystone identified for the joint equity topics in TCG-WPMU-2 was the protection of weapon components. The keystone identified for the four TCG-DS-2 topics was weapons of mass destruction development.

Recommendations

- Delete the ten DoD/DOS joint equity topics from TCG-WPMU-2. Delete the redundant DOE/DoD joint equity topic. Revise the classification level range from U-TSNSI to U-SNSI for one topic. Revise the declassification instructions for the two situation dependent topics to a 25-year duration.
- Retain the four topics in DS-2.
- Delete the single NSI topic in TCG-WI-2 and include a note to direct the derivative classifier to the appropriate guide for non-nuclear component shipments.
- Delete the single NSI topic in TCG-SAFF-2, because it will be sufficiently addressed in TCG-WPMU-3.
- Retain the single topic in TCG-VH-2.

Overall, this effort will result in a 40 percent reduction in the number of NSI topics in these five joint classification guides.

Working Group 26 – Improvised Nuclear Devices

Current Policy

The Department of Energy (DOE) National Nuclear Security Administration issues guidance to classify information associated with the theory, development, design, manufacture, fabrication, and assembly of improvised nuclear devices (INDs). The vast majority of the IND guidance addresses information categorized as Restricted Data under the Atomic Energy Act of 1954, as amended; however, there exist a limited number of IND-related activities that are appropriately classified under Executive Order 13526 as National Security Information (NSI).

Background

An IND is defined as a simple, crude, and intuitive device that can produce a nuclear yield. Typically, this type of device would not be one created by a nuclear nation-state, but a terrorist group. An IND is considered to be a weapon of mass destruction which could present significant and continuing threat to the national security of the United States.

The *DOE Classification Guide for Improvised Nuclear Devices* (CG-IND-1) is a limited distribution guide and, therefore, not widely available to many derivative classifiers that require guidance concerning INDs. When CG-IND-1 was approved in October 2006, the signatories intended that a thorough review and rewrite of the guide would be conducted once the guide had been used to make classification determinations and after feedback was received from the users. The Fundamental Classification Guidance Review is being conducted concurrently with the rewrite of the guide.

CG-IND-1 contains five NSI topics.

Analysis

No unique keystones were determined to belong to this guide. Of the five NSI topics, three are based on topics in the *DOE Classification and UCNI Guide for Radiological Emergency Response* (CG-RER-1). These three topics were reviewed by Working Group 24, Radiological Emergency Response. A fourth topic related to the physical security information concerning DOE sites and facilities that store Special Nuclear Material (SNM) is addressed by the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4). The fifth topic was determined to no longer be necessary.

Recommendations

For the five NSI topics in CG-IND-1:

- Rewrite one topic so that it will reflect the current guidance upon which it is based (the safeguards and security of SNM) and be declassified at 25 years. This could be implemented by inserting a simple pointer to the current guidance.

- Delete three topics that relate to the CG-RER-1 render safe procedures, as they are adequately addressed in that guide.
- Add one topic that points to useful guidance on IND mock-up devices in CG-RER-1. This topic will provide direct guidance on mock INDs to be used for training purposes.
- Delete one topic concerning fabrication of an IND that has been determined to be obsolete.

By implementing these recommendations in CG-IND-2, the total number of NSI topics will be reduced from five to two.

Working Group 27 - Second Line of Defense (Cancelled)

The Second Line of Defense (SLD) Program works with international partners to deploy systems to enhance host country capabilities to detect, deter, and interdict illicit trafficking in nuclear and other radiological materials. A working group has been established to develop a classification guide for the SLD program. Because the classification has not been completed, it is not appropriate to include this report. The DOE OC will ensure the guide is compliant with Executive Order 13526 as it is developed.

Working Group 28 – Weapons Two

Current Policy

The Department of Energy (DOE)/National Nuclear Security Administration (NNSA) issues guidance to classify information associated with weapon concepts that involve the use of a nuclear explosive as either the driver or in a directed energy device. Also, the DOE/NNSA issues guidance to classify information associated with testing of nuclear components in a manner that uses special nuclear material (SNM), but does not create a critical mass.

Background

Four classification guides were reviewed; two on energy weapons and two on testing of components not involving a critical mass. The Weapon Two guides on energy weapons included:

- The *Joint DOE/DoD Classification Guide for Nuclear Directed Energy Weapons* (CG-NDEW-2) which pertains to classification guidance related to the canceled Strategic Defense Initiative (SDI).
- The *Joint DOE/DoD Classification Guide for Directed Nuclear Energy Systems* (CG-DNES-2) contains guidance on information related to directed energy beams driven by a controlled (non-explosive) nuclear energy source.

Guides on the testing of nuclear components that use SNM but do not assemble a critical mass included:

- The *Joint DOE/DoD Topical Classification Guide for Non-Nuclear Testing* (TCG-NNT-2) which contains guidance on information for nuclear weapon testing not involving an actual nuclear explosion.
- The *DOE Classification Guide for Subcritical Experiments* (CG-SCE-1) contains guidance on information associated with experiments typically performed at the Nevada National Security Site in an underground facility.

Analysis

The working group identified four keystones. One sensitive keystone for CG-NDEW-2 and three sensitive keystones for CG-DNES-2. National Security Information (NSI) topics were either jointly owned equities of the DOE/NNSA and the Department of Defense (DoD) or topics uniquely owned by the DOE/NNSA or the DoD. Declassification instructions for topics uniquely owned by the DoD read as "See appropriate DoD guidance."

The topics uniquely owned by the DoD provide challenges to the users of the guides as these topics refer with the statement "See appropriate DoD guidance." These classification instructions were found to be outdated, as most of these programs were long ago canceled and no points of contact were identified.

Preliminary analysis of these four guides revealed:

CG-NDEW-2 – contained five NSI topics. Three topics were referred to "appropriate DoD guidance." Two of the three topics provided classification ranges, with no further delineation between classification levels. One topic involved the platform design requirements for an NDEW, which was referred to DoD for resolution. None of these three DoD topics were found to be exempt from automatic declassification at 25 years.

Two joint equity topics related to advanced energy conversion, which is defined to be "concepts, designs, and theories to convert nuclear weapons into a power source for another type of weapon." The two joint topics were exempt from automatic declassification at 25 years, as the release of such information would reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system, with a classification duration of 50 years.

CG-DNES-2 – contained 26 topics. Twenty topics represented joint equities. Three topics were equities of the DOE/NNSA, and three topics were equities of the DoD. All 26 topics were exempt from automatic declassification at 25 years, as the release of such information would reveal information that would impair the application of state-of-the-art technology within a U.S. weapons system, with a classification duration of 50 years.

For additional analysis, the 26 topics were grouped into three subject areas:

- *DNES effort* (3 topics). This includes information such as programmatic effort, budgets, to potential breakthroughs.
- *Advances in DNES technologies* (9 topics). Theoretical or experimental studies that could be used in a unique weaponizible way, such as a particularly useful lasing medium, design, or technological advance.
- *Military requirements of a DNES system* (14 topics). The military requirements can reveal the direction a technology must take to be effective, also the specifications of what constitute an effective weapon can reveal classified requirements or a classified objective of a DNES system.

TCG-NNT-2 – contained 13 topics; ten topics represented joint equities. Three topics were equities of the DoD. Of the 13 topics, 6 provided event-driven declassification instructions. Seven topics provided instructions for declassification at 25 years.

Five topics were determined to be not useful as written. The topics required the classifier to seek out other appropriate guidance; however, no guidance was specified. Also, these topics seemed to conflict with similar topics in the *Joint DOE/DoD Topical Classification Guide for Vulnerability and Hardening* (TCG-VH-2).

CG-SCE-1 – contained six topics. Five topics are based on topics in other guides involving SNM protection; one refers to information that is the equity of the United Kingdom (UK). The UK related topic was reviewed as a part of Working Group 37, U.S./UK equities. All six topics contain event-based declassification instructions.

Recommendations

The following recommendations were made:

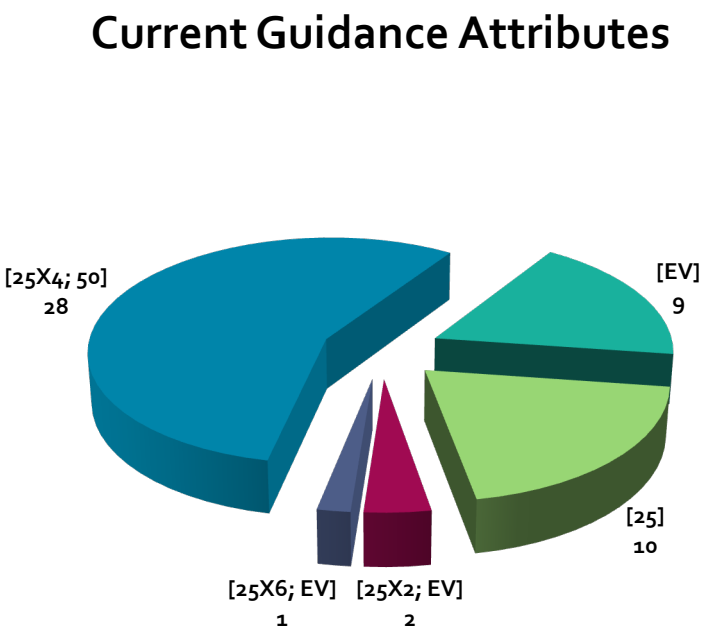
CG-NDEW-2: Remove the three topics addressing DoD equities and address them in the Broad Guidance. Modify the declassification instructions for the two topics addressing advanced energy conversion systems to be exempt from automatic declassification at 50 years, because release of such information would reveal key design concepts of WMD (50X2-WMD).

CG-DNES-2: Rewrite one topic related to the DNES program effort to conform to current guidance structure as the topics provided no clear guidance for a reviewer, ranging from Unclassified to Secret. Retain three topics that address DoD equities, and retain their current declassification instructions (25X4; 50). Modify the declassification instructions for the nine topics addressing advanced DNES technologies and the 14 topics regarding DNES military requirements to be exempt from automatic declassification at 50 years, because release of such information would reveal key design concepts of WMD (50X2-WMD).

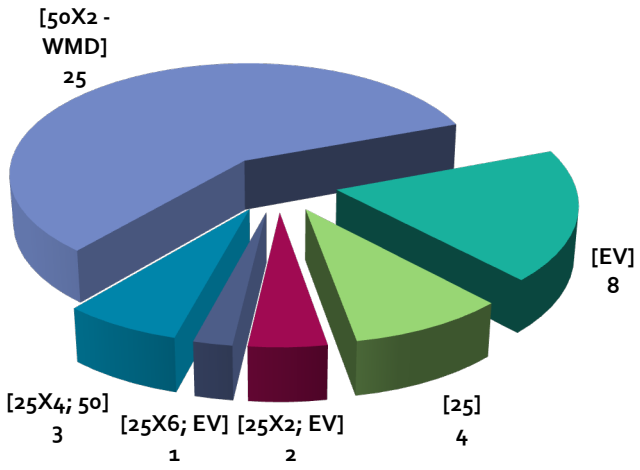
TCG-NNT-2: Retain two topics as written. Rewrite seven to conform to the current structure of the DOE's Office of Classification guidance as the topics provide no clear guidance for a reviewer, ranging from Unclassified to Secret. Remove four topics addressing DoD equities and address them in the Broad Guidance. Revise four topics to be consistent with TCG-VH-2. Delete one topic based on another agency's guide and replace with an appropriate note. The current declassification instructions should be retained for all topics with declassification events.

CG-SCE-1: Update topics as necessary at the conclusion of other working group efforts.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 29 – Testing

Current Policy

The Department of Energy (DOE) maintains several classification guides related to nuclear weapon testing.

Background

The *DOE Classification Guide for Nuclear Explosion Monitoring* (CG-NEM-1) is used primarily by personnel who have nuclear explosion monitoring responsibilities, but are not directly involved in day-to-day operations. The *Joint DOE/Department of Defense (DoD) Classification Guide for Safeguard C* (CG-SGC-1) is used as a basis for determining the level of classification of information concerning planning, support or execution of nuclear test operations and review of historical documents related to Safeguard C, which is the maintenance of the basic capability to resume nuclear testing in the atmosphere should it be deemed essential to national security. The guide also contains topics for the unlikely event of resumption of nuclear testing under the Safeguard C regime. The *Joint DOE/DoD Topical Classification Guide for Weapon Testing* (TCG-WT-1) is limited to the classification of information related to nuclear weapon testing.

Analysis

CG-NEM-1 contains 60 National Security Information (NSI) topics representing equities belonging to the Air Force Technical Applications Center (AFTAC). All topics are exempted from automatic declassification. The Office of Classification requested the assistance of the DOE Assistant Deputy Administrator for Nonproliferation Research and Development and AFTAC to review the topics in CG-NEM-1 against Executive Order (E.O.) 13526 requirements. The response from AFTAC provided links from CG-NEM-1 to their current guidance.

CG-SGC-1 contains 42 NSI topics representing equities belonging to the DoD, through the Defense Threat Reduction Agency (DTRA). Five of these topics refer to Department of State or DTRA guidance for declassification instructions, 7 topics have a 25-year declassification, and 30 topics have an event driven declassification. The Office of Classification requested the assistance of DTRA to review the guidance in CG-SGC-1 against E.O. 13526 requirements. DTRA recommended that 37 topics be retained as is, 4 topics be retained with revised declassification instructions to have a 50X2-WMD, and the one remaining topic be retained with declassification instructions changed to 25X2; 50.

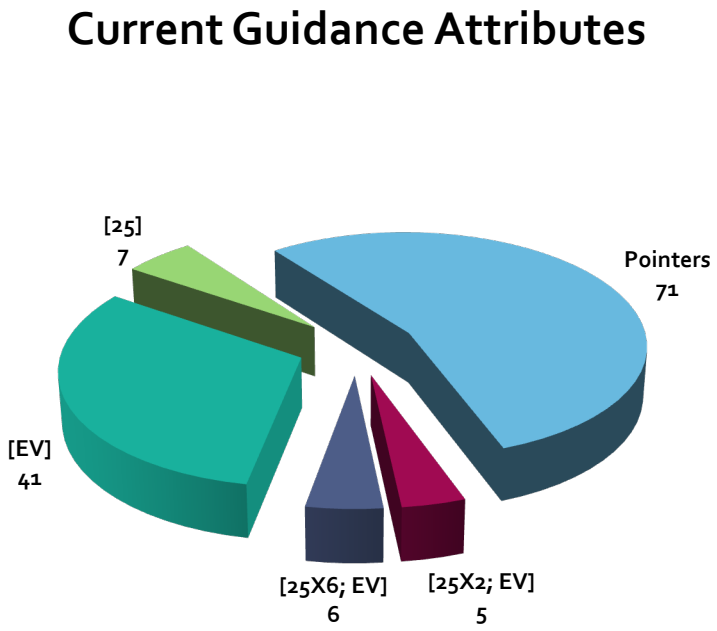
TCG-WT-1 contains 28 NSI topics representing equities shared between DOE and DoD. Of those, 15 are exempted from automatic declassification but have an event-driven declassification, one topic points to another guide (CG-ACVT-1), one topic refers to another agency (DTRA), and 11 have an event-driven declassification. Of the 15 topics exempted from automatic declassification, four are based on another classification guide (CG-NEM-1). The Office of Classification has requested the assistance of DoD to review the guidance in TCG-WT-1 for their equities against E.O. 13526 requirements.

There are no unique DOE keystones.

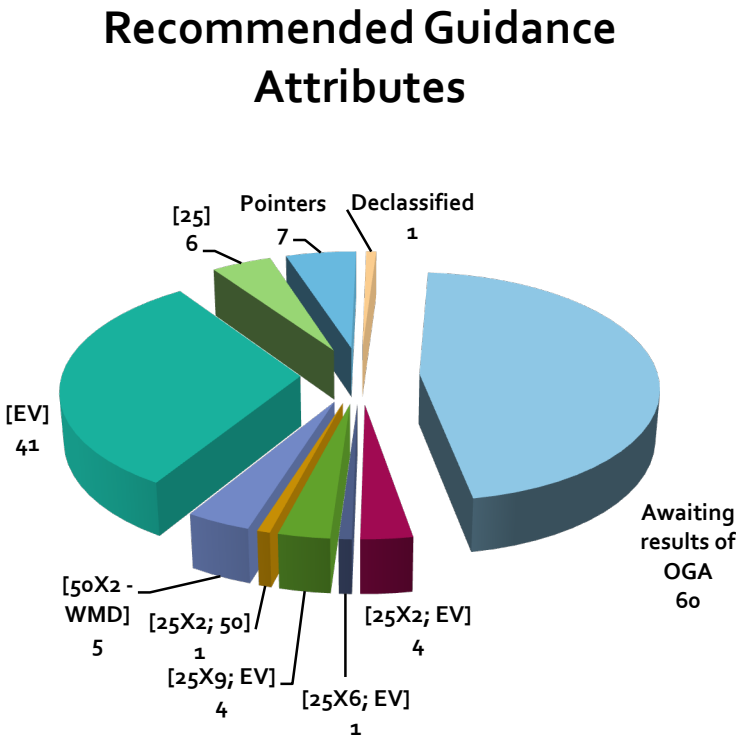
Recommendations

- Revise CG-NEM-1 when AFTAC has completed its Fundamental Classification Guidance Review.
- Incorporate DTRA's recommendations into CG-SGC-1.
- For TCG-WT-1, one topic needs to be revised to reflect WNP-114 (*Meteorological Restrictions at the Nevada Test Site*), the topics that are based on or point to other guidance will be revised when that guidance has been revised, the declassification instructions for the four topics protecting United Kingdom equities will be changed from 25X6; EV to 25X9; EV, and the remainder of the topics will be retained as is. One topic is recommended to have its declassification instruction changed to 50X2-WMD.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 30 – Civilian Radioactive Waste

Current Policy

The *Joint DOE and NRC Sensitive Unclassified Information and Classification Guide for the Office of Civilian Radioactive Waste Management Program* (CG-OCRWM-1) provided guidance on classified and sensitive unclassified information associated with the DOE Office of Civilian Radioactive Waste Management's program for constructing and operating a geologic repository for the disposal of spent nuclear fuel and high-level radioactive waste at Yucca Mountain, Nye County, Nevada.

The *Joint DOE/NRC/DOT/DHS Classification and Sensitive Unclassified Information Guide for the Transportation of Radioactive Waste to Yucca Mountain* (CG-RWT-1) provided guidance on sensitive unclassified information and classified information associated with the DOE Office of Civilian Radioactive Waste Management (RW) program, and the RW Transportation System for the transport of non-Naval spent nuclear fuel and high-level waste to Yucca Mountain.

Background

The budget for the geologic repository for the disposal of spent nuclear fuel and high-level radioactive waste at Yucca Mountain, Nye County, Nevada, was eliminated.

Analysis

CG-OCRWM-1 contained 80 NSI topics and CG-RWT-1 contained 78 NSI topics.

In correspondence dated July 26, 2011, the Office of Classification requested that the Nuclear Regulatory Commission (NRC) review CG-OCRWM-1 per section 1.9 of EO 13526 and either concur with the DOE recommendation to cancel the guide or to proceed with a working group to update the guide to comply with the Executive order. NRC concurred with cancellation of the guide.

In correspondence dated July 26, 2011, the Office of Classification requested that the NRC, Department of Transportation (DOT), and Department of Homeland Security (DHS) review CG-RWT-1 per section 1.9 of EO 13526 and either concur with the DOE recommendation to cancel the guide or to proceed with a working group to update the guide to comply with the Executive order. NRC, DOT, and DHS concurred with cancellation of the guide.

Recommendations

With the concurrence of the other agencies and the DOE program office, CG-OCRWM-1 and CG-RWT-1 were cancelled. If the program were to be restarted, the need for a specific program classification guide would be revisited.

Summary of Topics Reviewed

Per correspondence dated October 18, 2011, CG-OCRWM-1 was cancelled. Documents created after the date of cancellation will be reviewed for classification using the applicable agency classification guidance. Historical documents will be referred to the originating agency for classification review for purposes of declassification or downgrading.

Per correspondence date October 18, 2011, CG-RWT-1 was also cancelled. As with CG-OCRWM-1, documents created after the date of cancellation will be reviewed for classification using the applicable agency classification guidance and historical documents will be referred to the originating agency for classification review for purposes of declassification or downgrading.

As of the cancellation of these two guides, 158 topics have been deleted.

Working Group 31 - Weapons One

Current Policy

Four DOE classification guidance documents addressing nuclear weapons were identified for review.

Background

The *Joint DOE/DoD Nuclear Weapon Classification Policy Guide* (CG-W-5) provides information concerning the classification to be assigned to information about the development, design, manufacture, or use of nuclear weapons. The *Topics Retained from the Joint DOE-DoD Nuclear Weapons Classification Guide* (CG-W-4, Rescission) provides similar information as CG-W-5. The *Joint DOE/DoD Topical Classification Guide for Nuclear Weapon Use Control* (TCG-UC-3) provides guidance concerning the classification of positive measures that, given access to a nuclear weapon, permit the authorized use and prevent or delay the unauthorized use of nuclear weapons. The *Joint DOE/DoD Topical Classification Guide for Nuclear Weapon Materials* (TCG-WM-2) provides information concerning the classification of materials used in the DoD and DOE for research, development, testing and production of nuclear weapons.

Analysis

- CG-W-4, Rescission, contains 9 NSI topics representing equities belonging to the DoD.
- CG-W-5 contains 10 NSI topics that point to topics in other guides.
- TCG-UC-3 contains 11 NSI topics representing equities belonging to either the DoD (5 topics) or the NSA (6 topics).
- TCG-WM-2 contains 3 NSI topics representing equities belonging to the United Kingdom.

Because all NSI topics represented equities of other agencies or point to topics in other guides, additional analysis was not required. There are no unique DOE keystones.

Recommendations

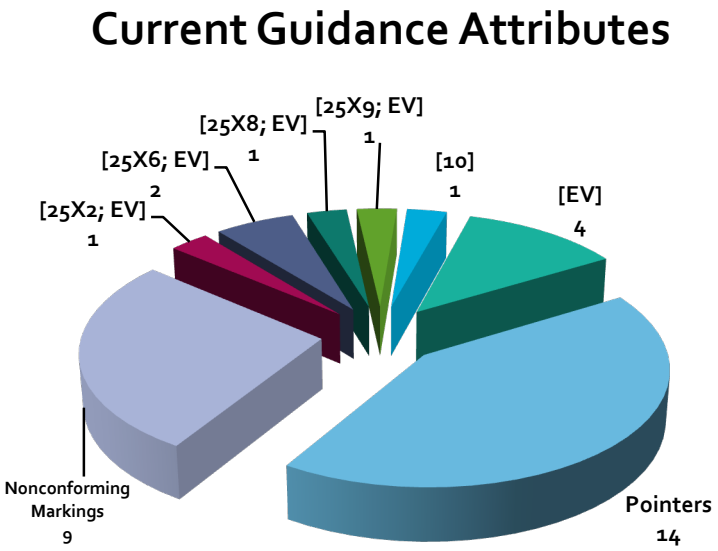
Delete the 9 NSI topics from CG-W-4 and migrate all other topics into a revision of CG-W-5. Cancel CG-W-4. *On January 18, 2012, CG-W-5, Change 14, was approved.* With this change CG-W-4 was cancelled.

Update all NSI topics in CG-W-5 that refer to other guides to be consistent with their basis topics found in TCG-WPMU-2, TCG-WT-1, and WNP-122. *On January 18, 2012, CG-W-5, Change 14, was approved.* Changes included updates to reflect the current guidance in TCG-WPMU-2, TCG-WT-1, and WNP-122, and one topic was deleted.

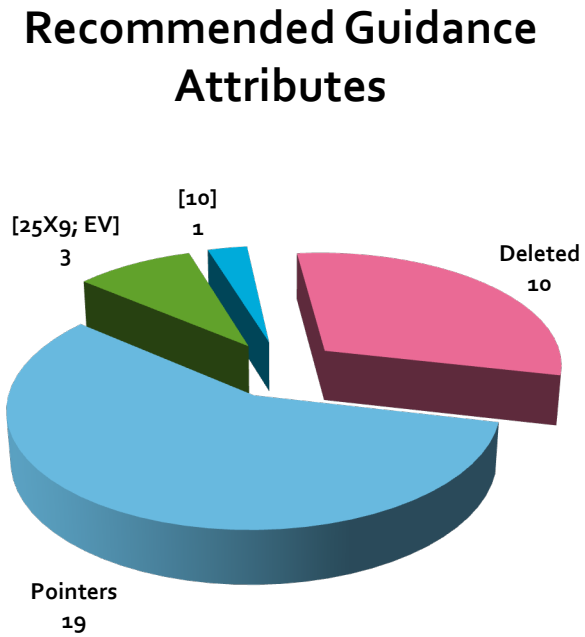
In next change to TCG-UC-3, delete the note requested by NSA. *Change 5, TCG-UC-3, is final concurrence.*

In next change to TCG-WM-2, change the declassification instructions for the NSI topics to be consistent. Recommended declassification instruction is: "[25X9; EV] Declassification of this information will be based on the provisions of the 1958 U.S. - UK Mutual Defence Agreement and will be implemented upon agreement of the U.S. and the UK to declassify."

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 32 - Radiation Hardened Microelectronics

Current Policy

DOE in conjunction with the Department of Defense maintains a classification guide related to the radiation hardening of microelectronics.

Background

The *Joint DOD-DOE Radiation Hardened Microelectronics Guide* provides a basis for determining levels of security classification to be assigned to information concerning the design, processing, fabrication, and testing of electronic devices that are hardened to withstand the effects of radiation environments. The continued availability of radiation hardened microelectronics and the technologies used harden microelectronic devices is a key element of national security for DoD space and missile systems to include nuclear weapons. The guide had not been updated since January 1989 and was not in compliance with the Executive order. As a result, a classification working group was convened in December 2009 to revise the *Joint DOD-DOE Radiation Hardened Microelectronics Guide*. The FCGR was conducted concurrently with the rewrite of this guide.

Analysis

A total of 38 NSI topics were reviewed. Of those topics,

- 21 had no declassification instructions.
- 17 had declassification instructions of "Originating Agency's Determination Required."

As a whole, the topics did not reflect technologies now published in the commercial sector. The use of radiation hardening techniques to achieve high levels of immunity has been widely published in the commercial sector as have the partial details of radiation hardening by process approaches. Thus, the guidance to control the distribution of piece-part radiation hardening technical data must be cognizant of the existing open literature.

The specific keystones being protected by classification are: (1) system level hardness and vulnerabilities, and (2) unique design details and material improvements that are not commercially available.

Recommendations

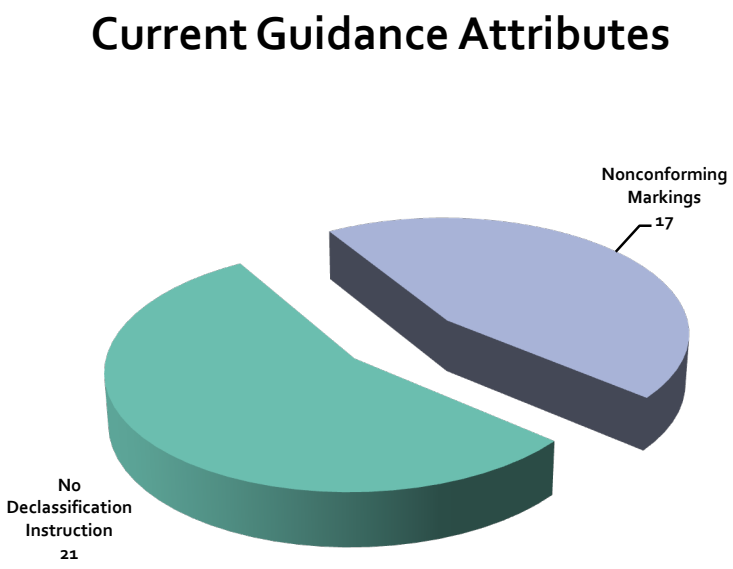
Twenty-eight topics had their classification retained and the declassification instructions were rewritten to be compliant with Executive Order 13526. Six topics were deleted by combining them with other topics. A chapter with one new NSI topic was added to cover the classification of information related to neutron-induced displacement damage. Three topics were recommended for declassification. One topic was recommended for declassification in part. Three topics were recommended to have the classification upgraded, in order to resolve a

shortcoming in the classification of energy disposition from classified sources and promising techniques for elimination devices that fail at low thermo-mechanical stress levels. In total:

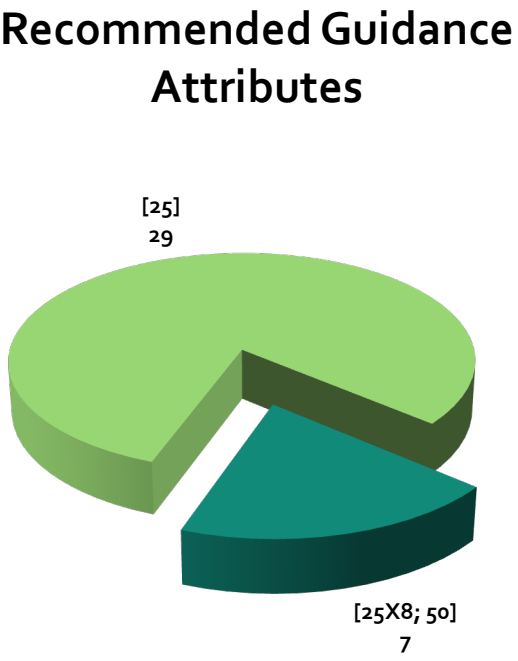
- 7 topics were determined to be exempt from automatic declassification at 25 years, with instructions to declassify at 50 years.
- 25 topics with instructions to declassify at 25 years.

Because the original classification authority for this NSI is under the purview of the DoD, the recommended changes in classification and declassification instructions were approved by DoD in revised guidance (CG-MIC-1) dated October 19, 2011 and approved by DOE on November 17, 2011.

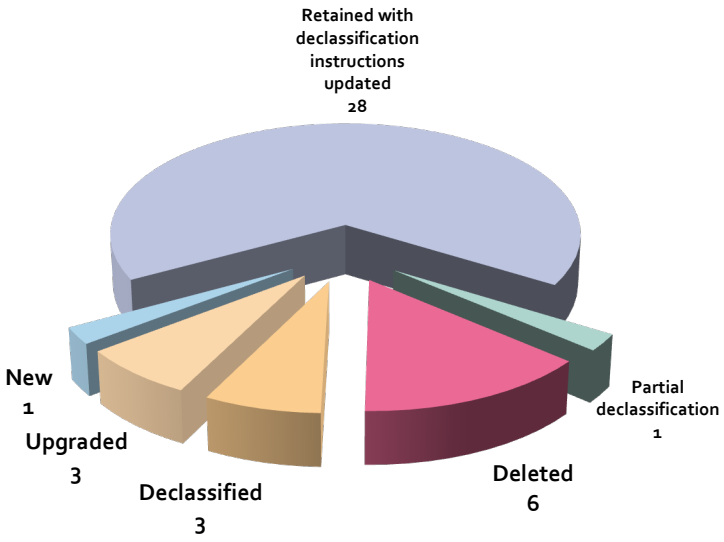
The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



This chart summarizes the result of the review:



Working Group 33 – Treaties

Current Policy

Classification guidance is required for the Department of Energy (DOE) Office of Nuclear Verification to accomplish activities in the area of treaty negotiation as well as to support activities to evaluate treaty compliance and treaty verification technologies.

Background

Four classification guides were identified for review. These guides were grouped together due to their relationship to programs pertaining to treaty development, negotiation, and verification. Many of these topics address equities shared between the DOE, Department of Defense (DoD), and Department of State (DOS); however, some address equities solely belonging to the DOS.

The four classification guides identified for review are:

- The *DOE Classification and UCNI Guide for Arms Control and Verification Technology* (CG-ACVT-1) addresses information related to arms control treaties and the technologies used to ensure treaty compliance by other countries.
- The *Joint DOE/DoD Classification Guide for Arms Control Negotiations* (CG-ACN-1) addresses information related to treaty protocols, options and negotiating positions, as well as assessments of reactions by other countries to these options.
- The *Classification Guide for Plowshare Program and Treaty Verification* (CG-PPTV-1) addresses information pertaining to peaceful uses of nuclear weapons (primarily the Plowshare Program) and identified information that has been declassified about the program.
- The *DOE Classification Guide for Nonproliferation of Weapons Information* (CG-NP-3) addresses information pertaining to nuclear nonproliferation treaties that are negotiated between the U.S. and foreign governments.

Analysis

The keystones identified are:

- Treaty negotiation stances that maintain and maximize outcome.
- Technical details which, if known to a treaty party, would allow circumvention of detection and verification protocols.

CG-ACVT-1 – Contains one hundred and three National Security Information (NSI) topics; 30 refer to other topics within the guide or other guides; 27 represent equities belonging to other agencies; and 46 represent equities shared between DOE, DOS, and DoD. For the 46 shared equity topics:

- Forty four topics are exempt from automatic declassification at 25 years and have event-driven declassification instructions.
- Two topics have event driven declassification instructions.

In most cases, the event for all topics identified above is "when jointly approved" by the owning agencies. These events were determined to be the appropriate declassification instructions.

CG-ACN-1 – Contains 31 NSI topics. Of those topics:

- Twenty-four refer to topics in the *Classification and UCNI Guide for Safeguards and Security Information* (CG-SS-4). These CG-SS-4 basis topics were reviewed by other working groups.
- Three refer to other topics within the guide.
- Two topics describe equities shared between DOE and DOS, and are exempt from automatic declassification at 25 years, with event driven declassification instructions ("when jointly approved" by DOE and DOS). These events were determined to be the appropriate declassification instructions.
- Two topics referring the information to DOS.

CG-PPTV-1 – Contains ten NSI topics. Of those topics:

- One refers to another topic within the guide.
- Five represent equities belonging to other agencies.
- Four describe equities shared between DOE and DOS. These four topics address information exempt from declassification at 25 years. The four topics have event driven declassification instructions ("when jointly approved" by DOE and DOS). These events were determined to be the appropriate declassification instructions.

CG-NP-3 – Contains 33 NSI topics.

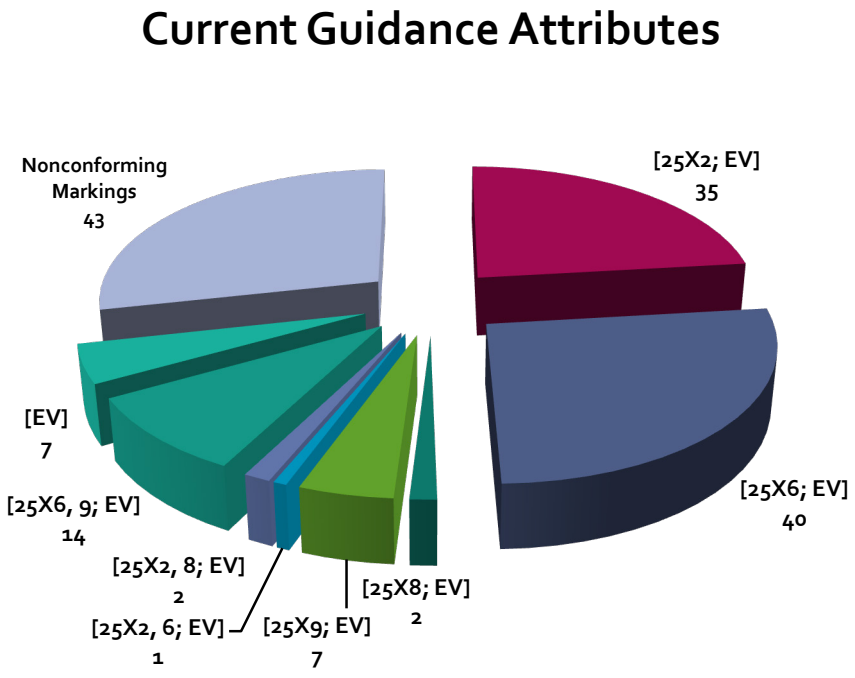
- Nine refer to other topics within the guide.
- One represents an equity belonging to another Government agency.
- Twenty-three represent equities shared between DOE and DOS. The topics are exempt from declassification at 25 years and have event driven declassification instructions ("when jointly approved" by DOE and DOS). These events were determined to be the appropriate declassification instructions.

Considering the four guides overall, the program office confirmed that the protection of negotiating positions and subsequent analysis represents information critical to national security, because future treaty approaches and methodologies depend in large part on past treaties. Furthermore, even if many of the techniques and methodologies used to monitor treaty compliance are well known and publicly available, the specific positioning by DOS, DoD, and DOE should be classified to protect leverage of positions as well as future negotiating stances, thereby justifying the exemption from automatic declassification at 25 years. These topics should remain event driven, with declassification only when jointly approved by the cognizant agencies.

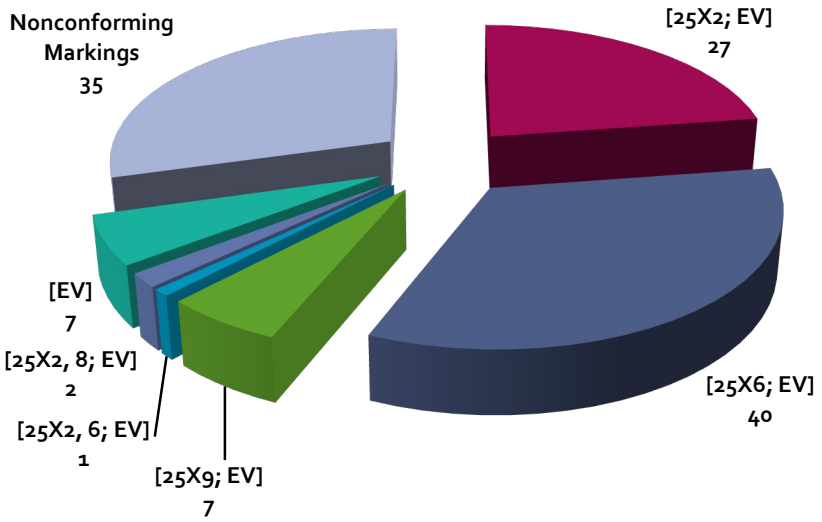
Recommendations

- Maintain the 25X exemptions now stated in the existing guides.
- Delete topics in CG-ACN-1 that refer to CG-SS-4 topics related to physical security issues at DOE sites, and refer the derivative classifier to the relevant topics in CG-SS-4 or subsequent guides.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 34 – Chemical/Biological Programs

Current Policy

The Department of Energy's (DOE) work related to chemical and biological (C/B) agents is part of the work for others program where other Federal agencies and non-Federal organizations can take advantage of DOE's expertise. The work in this area consists of focused technology development for facility protection and a broad-based research and development program, purely defensive in nature, with the goal of reducing the threat of C/B weapons of mass destruction. This program encompasses information, technologies, and systems that may be used to prevent, detect, mitigate, or otherwise defensively respond to the threatened or actual use of chemical or biological weapons.

Background

The *Classification Guide for Chemical/Biological Defense Information* (CG-CB-2) addresses information about development, use, deployment, defeat and destruction of chemical and biological agents. The guide was developed for the DOE laboratories to be used in accomplishing work for customers within the laboratory, and for external customers requesting laboratory expertise through the WFO program. These external customers may not have adequate classification guidance for their programs related to C/B activities.

Analysis

Keystone:

- Protect development, production, and use of C/B WMD.

In CG-CB-2, fifty National Security Information (NSI) topics were identified. Seven refer to other topics within the guide; 26 address information that is the equity of other agencies (only seven topics have declassification instructions), and 17 topics address unique DOE equities. Of those 17 topics:

- Seven topics are exempt from automatic declassification at 50 years. These 7 topics had an incorrect declassification instruction of Secret (S) NSI [25X2; 100].
- Two topics are exempt from automatic declassification at 25 years and have event based declassification instructions.
- Eight topics require declassification at 25 years.

Information concerning the detection and destruction of C/B agents was considered less of a security risk because developments in these areas are driven more by commercial developments and technologies and benefit is realized through exchanges with these commercial entities and, therefore, a classification level of S and a duration of 25 years is sufficient.

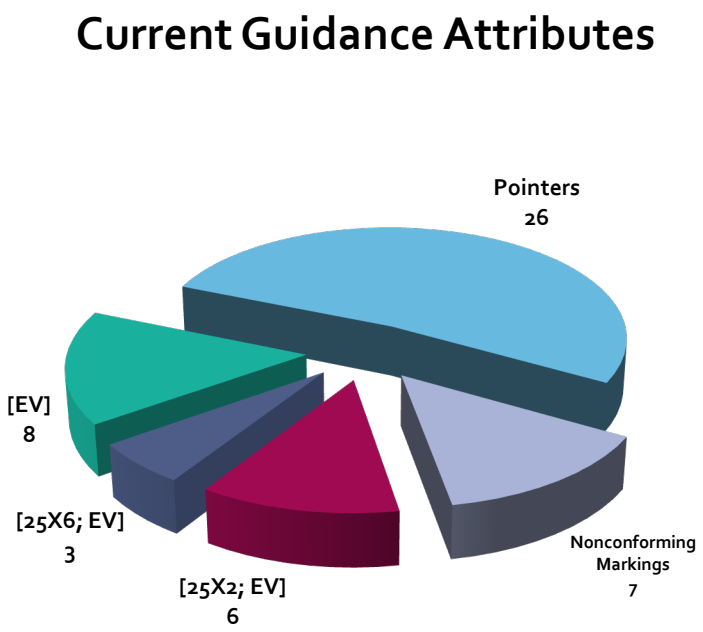
The two topics citing 25X2 durations were changed to declassification instructions at 50 years. These two topics related to the inability to detect an agent, and modeling activities. Fifty years

was determined to be an adequate duration of classification due to independent advancement in these areas.

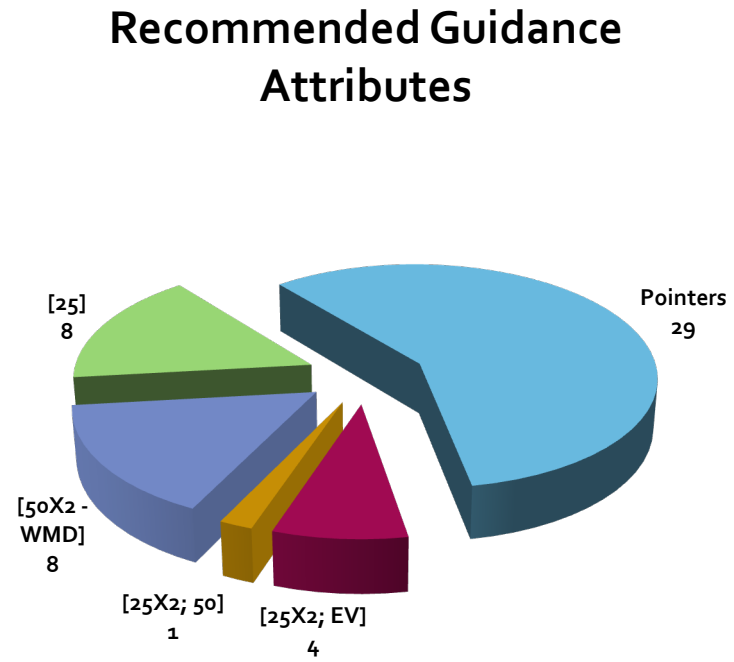
Recommendations

- Revise the topics related to agent and dispersal information to be exempt from declassification at 50 years. This will affect 8 topics (7 with the incorrect declassification instructions of [25X2; 100] and the one topic with the [25X2; EV] declassification marking), changing the classifications to SNSI [50X2 – WMD].
- Revise the topics related to detection and destruction technologies to declassify the information at 25 years. This will affect 8 topics.
- Change 1 topic with a [25X2; EV] to [25X2; 50].
- Revise 3 topics that are clearly another agency's equity from [25X2; EV] to [refer]. The animal use topics fit this and the 3 topics affected should be changed to Confidential NSI (refer).
- Retain 4 remaining other agency equities as is.

The following chart identifies the declassification events used in the current guidance:



The following chart identifies the changes from the current guidance:



Working Group 35 - NA-20

Current Policy

A diverse group of classification guides addresses the classification of verification methodologies developed and used by the Department of Energy (DOE) in support of non-proliferation activities, treaty monitoring and other activities as defined by the National Nuclear Security Administration, Office of Defense Nuclear Nonproliferation (NA-20). These technologies are used to directly and indirectly monitor signatures of nuclear activities in countries of a proliferation concern.

Background

Six classification guides were identified for review, based on program agency involvement. These guides are:

- The *Chemical Analysis by LASER Interrogation of Proliferation Effluents Program* (CALIOPE) guide classifies lasers and detection methods used to identify and characterize effluents emitted by nuclear proliferation activities.
- The *Classification Guide for Remote Ultra Low Light Imaging* (CG-RULLI-1) classifies information for the RULLI program that used "single photon" imaging of light signals to assist in determining phenomena that could be associated with clandestine nuclear activities.
- The *Joint DOE/DoD Classification Guide for the Nuclear Test Detection Satellite (Project VELA and VELA Follow-On)* (CG-WV-5) classifies information in Project VELA and the VELA Follow On programs, that were terminated in September 1984. The program used radiation monitoring technologies to detect nuclear weapon tests.
- The Cibola Flight Experiment program (CG-CFE-1) has the primary mission of testing a reconfigurable processor payload intended for Low Earth Orbit to further the technology for detecting nuclear electromagnetic pulse (EMP).
- The *Classification Guide for the Beacon Program* (CG-BP-1) classifies information associated with the Beacon Program, which used imaging technologies to identify ground activity that could be associated with clandestine nuclear activities.
- The *Classification Guide for the Multi Spectral Thermal Imaging (MTI) Program* (CG-MTI-1) classifies information in a program that uses thermal imaging of the ground to identify variations that would indicate potential nuclear proliferation activities.

Analysis

The keystones identified are:

- Treaty negotiation stances that maintain and maximize outcome.
- Technical details which, if known to a treaty party, would allow circumvention of detection and verification protocols.

Refer to the classified appendix for additional information.

Analysis of the six guides revealed:

- CALIOPE – Sixteen National Security Information (NSI) topics; two refer to other topics within the guide and 14 address equities of another U.S. Government agency.
- CG-RULLI-1 – Nineteen NSI topics; three refer to other topics within the guide and 16 address equities of another agency.
- CG-WV-5 – Ninety-three NSI topics; 16 refer to other topics within the guide. The remaining 77 topics address equities of other agencies. None of the topics in the guide had declassification instructions.
- CG-CFE-1 – Eleven NSI topics that address equities of other agencies.
- CG-BP-1 – Thirteen NSI topics that address equities of another agency. None of the topics in the guide had declassification instructions.
- CG-MTI-1 – Forty-one NSI topics; 8 refer to other topics within the guide and 26 address equities of another agency. The remaining seven address equities shared between DOE and another agency. All seven topics are exempt from automatic declassification at 25 years, with event based declassification instructions. The declassification event is "when the information no longer assists adversaries." Nine topics in this guide did not have declassification instructions.

Of the seven joint equity topics in CG-MTI-1, three involve DOE sites that directly support the NA-20 program, and the remaining four pertain to MTI performance information that could reveal techniques to counter the ability to measure treaty non-compliance. It was determined that satellite technologies, including the performance of the MTI satellite, are continuing to evolve; thus a classification duration of 50 years is adequate.

Recommendations

- Integrate these six individual program guides into one general guide, containing individual chapters to address specific information about each program. The consolidation would reduce the number of individual guides requiring management, and guidance required by the NA-20 program office would be available in one location.
- Revise the seven joint equity topics in CG-MTI-1 to require automatic declassification at 50 years.
- Because the topics relate primarily to equities of another agency, review the guides for necessary revisions after the other agency has completed their Fundamental Classification Guidance Review activities.

Working Group 36 – High Power Radio Frequency

Current Policy

The High Power Radio Frequency Program (HPRF) relates to an Air Force program whose purpose was to utilize a nuclear weapon to drive a source or fixture to produce high energy output for defense purposes. The Defense Threat Reduction Agency (DTRA) is the oversight office for such programs, and the Air Force Nuclear Weapons Center (AFNWC) is the owner of the program. The HPRF program never resulted in any design of a system to perform as an HPRF source - all activities ended in the mid-1990s.

Background

Classification guidance addressing this program is contained in one DOE guide, the *Classification Guide for High Power Radio Frequency (HPRF) Program* (CG-HPRF-2). The guide was generated in the 1990s to support the HPRF program, which was intended to investigate the design of a system that could provide high-level energies for use against an adversary.

Analysis

The guide contains seven National Security Information (NSI) topics. All NSI topics were determined to address equities belonging to the AFNWC. After review, it was confirmed that all DOE information being protected is adequately identified in other joint DOE/DoD Topical Classification Guides (TCG) or DTRA guides which base the classification requirements on the TCGs. The TCGs for Nuclear Assembly Systems, Use Control and Vulnerability/Hardening are the guides which contain the topics necessary to protect the DOE information contained in the CG-HPRF-2 Classification Guide.

Recommendations

- Transfer responsibility for the NSI topics in this guide to the AFNWC.
- Cancel CG-HPRF-2 once the AFNWC has accepted responsibility for the NSI topics.

Working Group 37 – United Kingdom

Current Policy

The United States and the United Kingdom signed a treaty in 1958 to share certain information about nuclear materials production and nuclear weapons development. Known as *The Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America for Co-operation on the Uses of Atomic Energy for Mutual Defence Purposes*, it has been revised on several occasions since issuance.

The classification guidance documents are:

- Classification bulletin GEN-17, *Association of U.K. and U.S. Nicknames* – addresses material nickname associations.
- The *DOE Classification Guide for Nuclear Materials Production* (CG-NMP-2), addresses the US and UK material Barter programs.
- *Joint DOE/DoD Topical Classification Guide for Nuclear Weapons Materials* (TCG-WM-2) – pertains to the same subject addressed by GEN-17.
- *Joint DOE/DoD Topical Classification Guide for Weapons Testing* (TCG-WT-1) – addresses UK participation in weapon testing.
- *DOE Classification Guide for Subcritical Experiments* (CG-SCE-1) – addresses UK participation in subcritical testing programs.
- *Joint Classification Guide for the Exchange and Safeguard of Materiel between the United States and the United Kingdom* (CG-UK-2) – addresses detailed information on the US and UK barter programs.
- *DOE Classification and UCNI Guide for Radiological Emergency Response* (CG-RER-1) – addresses information involving Radiological Emergency Response.
- *Joint U.S./UK Classification Guide for Nuclear Weapons* (CG-US/UK-NUC-1) – addresses nuclear weapons information exchanged between the US and the UK.

Background

Topics involving UK information equities were compiled from eight classification guidance documents. The number of topics range from two complete guides to a few topics, for a total of 76 topics. These topics are addressed as follows:

- Classification bulletin GEN-17, *Association of U.K. and U.S. Nicknames* – one topic with a declassification instruction of OADR.
- The *DOE Classification Guide for Nuclear Materials Production* (CG-NMP-2), two topics exempt from automatic declassification at 25 years (25X6) with event driven declassification instructions.
- *Joint DOE/DoD Topical Classification Guide for Nuclear Weapons Materials* (TCG-WM-2) – three topics exempt from automatic declassification at 25 years (25X6 and 25X9) with event driven declassification instructions.

- *Joint DOE/DoD Topical Classification Guide for Weapons Testing* (TCG-WT-1) – four topics exempt from automatic declassification at 25 years (25X6) with event driven declassification instructions.
- *DOE Classification Guide for Subcritical Experiments* (CG-SCE-1) – one topic exempt from automatic declassification at 25 years (25X6) with an event driven declassification instruction.
- *Joint Classification Guide for the Exchange and Safeguard of Materiel between the United States and the United Kingdom* (CG-UK-2) – Forty-two topics:
    - Twenty-nine topics exempt from automatic declassification at 25 years (25X9) with event driven declassification instructions.
    - Thirteen topics with event driven declassification instructions.
- *DOE Classification and UCNI Guide for Radiological Emergency Response* (CG-RER-1) – one topic exempt from automatic declassification at 25 years (25X6) with an event driven declassification instruction.
- *Joint U.S./UK Classification Guide for Nuclear Weapons* (CG-US/UK-NUC-1) – Twenty-two topics:
    - Twenty topics exempt from automatic declassification at 25 years (25X6) with event driven declassification instructions.
    - Two topics with event driven declassification instructions.

Analysis

One keystone was identified – protection of information belonging to the UK. Detailed analysis was provided to the responsible official in the UK, including the US recommendations concerning each topic. The response received from the UK confirmed that current classification levels and declassification instructions were adequate. However, the Office of Classification analysis concluded that the majority of the "25Xn" topics should be 25X9, not 25X6, because the information protected is subject to the US UK Mutual Defence Treaty. Only two appear to meet the criteria for exemption from automatic declassification based on E.O. 13526, Sec. 3.3 (b)(6) as Foreign Government Information.

The fifteen topics with event driven declassification instructions were determined to be correct, as they addressed shipment transportation information and do not meet criteria in Executive Order (E.O.) 13526 for exemption from declassification at 25 years. The one topic addressed by classification bulletin GEN-17 is redundant, as the information is adequately addressed in TCG-WM-2.

Recommendations

- Engage the UK responsible officials to confirm that 25X9 is the appropriate criterion for fifty-eight of the topics that meet the requirement in E.O. 13526, Sec. 3.3 (b)(9) and are treaty driven. Confirm with the UK that only two topics meet the criteria for exemption from automatic declassification based on E.O. 13526, Sec. 3.3 (b)(6) and should be 25X6.
- Delete classification bulletin GEN-17, as this topic is adequately addressed in TCG-WM-2. (Deletion of this bulletin requires UK concurrence).

Appendix J. List of DOE keystones

List of Keystones Identified During Review

Arms control
Assessed performance
Capabilities/limitations of the TSCM program.
CI identification
Date of service
Deficient Performance
Diversion detection threshold
Exploitable design information
Foreign facility – vulnerability
Foreign relations of the U.S. Government.
Hardening
HEU agreement information
Identification of a vulnerability/hazard.
Identification, design, or optimization of unique technologies for radiological dispersal or radiation exposure.
IND information
Information classified because of the enhanced security controls in place.
Information that could be exploited by an outside adversary to gain access to classified information on a system.
Information that reveals a link to a foreign intelligence service.
Information that would assist an adversary in acquiring classified information.
Information that would assist an adversary in acquiring material (SNM, a weapon, a part).
Information that would assist an adversary in planning or executing a successful attack by lowering the performance of a security system or component.
Intelligence sourced capability
Material verification
NCTIR defeat capability
NCTIR defeat vulnerability
NCTIR diagnostic capability
NCTIR diagnostic vulnerability
NCTIR modeling capability
NCTIR modeling vulnerability
NCTIR search capability
NCTIR search vulnerability
NCTIR tactic, technique, or procedure

Non-explosive RDD techniques

Novel method/technique

Planned response

Protection of information belonging to the UK.

Protection of information on development, production, and use of chemical or biological WMD.

Protection of weapon components.

Provocative information which might encourage an RDD/RED attack.

Requirement deficiency

Results of dispersal tests or experiments, and subsequent analysis.

SNM - Allocation

SNM – Packaging

SNM – Recovery

SNM – Safeguards

SNM – Transport

SNM - Vulnerable location

SNM safeguards of plutonium placed in deep boreholes.

Source identification

Space mission data

Space reactor design

Space reactor material

System level hardness and vulnerabilities

Targeting information

Targeting information that would be useful in planning an attack by identification of a shipment contents or the timing and location of a shipment.

Technical details which, if known to a treaty party, would allow circumvention of detection and verification protocols.

TFNI identification

The general methodology behind cover/disassociated procurements.

Treaty negotiation stances that maintain and maximize outcome.

Unique design details and material improvements that are not commercially available.

Weapons of mass destruction development

Twelve classified and four Official Use Only keystones are not listed.

Appendix K. Summary of DOE 50-year exemption memorandum to the Information Security Oversight Office

Summary of DOE Proposed 50X Exempted Information

In a letter, dated January 5, 2012, to the Interagency Security Classification Appeals Panel, DOE provided the following 10 proposals for the exemption of information in accordance with Executive Order (E.O.) 13526, section 3.3(j). These are types of information that DOE has determined require exemption from automatic declassification at 50 years. All identified areas of information pertain to key design concepts of weapons of mass destruction (WMD), as cited in E.O. 13526, Sec. 3.3 (h) (1) (B).

1) In the area of Transportation Safeguards Systems, topics describing the following concept require a 50X2-WMD exemption:

> *Design details and operating features that, if known, would aid in the defeat or bypass the Safe Secure Trailer (SST)*

2) In the area of Fixed Site Security Systems, topics describing the following concept require a 50X-2 WMD exemption:

> *Design details and operating features that, if known, would aid in the defeat or bypass of fixed site security features*

3) In the area of Chemical/Biological Weapons, topics describing the following two concepts require a 50X2-WMD exemption:

> *Classified Chemical/Biological agents or simulants or significant improvements in them*
>
> *Exploitable information about agent dispersal*

4) In the area of Radiological Dispersal Devices (RDD) and Radiation Exposure Devices (RED), topics describing the following three concepts require a 50X2-WMD exemption:

> *Identification, design, or optimization of unique technologies for radiological dispersal or radiation exposure*
>
> *Non-explosive RDD techniques*
>
> *Provocative information which might encourage an RDD or RED attack*

5) In the area of Nuclear Directed Energy Weapons, topics describing the following concept require a 50X2-WMD exemption:

> *Concepts, designs, and theories to convert a nuclear weapon into a power source for another type of weapon (i.e., Advanced Energy Conversion)*

6) In the area of Directed Nuclear Energy Systems (DNES), topics describing the following two concepts require a 50X2-WMD exemption:

> *Theoretical or experimental studies that could be used in unique weaponiziable ways, such as identification of lasing mediums or gases or solids (i.e., Advanced Materials Applications)*
>
> *Necessary characteristics of a weapon to achieve a specific military goal or application of the technology to achieve a specific military goal or application of the technology for a military purpose (i.e., Military Requirements)*

Appendix L. List of Acronyms and Abbreviations

List of Acronyms and Abbreviations

ACN	Arms Control Negotiation
AEC	Atomic Energy Commission
(C)	Confidential
CBP	Customs and Border Protection
CFR	Code of Federal Regulations
CG	Classification Guide
CGS	Classification Guidance System
CI	Counterintelligence
CII	Critical Infrastructure Information
CNSI	Classified National Security Information
COMSEC	Community Security
DBT	Design Basis Threat (replaced with GSP)
DC	Derivative Classifier
DD	Derivative Declassifier
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOE	Department of Energy
DOT	Department of Transportation
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FGI	Foreign Government Information
FCGR	Fundamental Classification Guidance Review
FIS	Foreign Intelligence Service
FRD	Formerly Restricted Data
GSP	Graded Security Protection
HSS	Office of Health, Safety and Security
HQ	Headquarters
HUM	Human Confidential or Intelligence Source
IC	Intelligence Community
IN	Intelligence
IND	Improvised Nuclear Device
ISOO	Information Security Oversight Office
MPP	Material Protection Project
NA-20	National Nuclear Security Administration, Office of Defense Nuclear Nonproliferation
NA-42	National Nuclear Security Administration, Office of Emergency Response
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSI	National Security Information
OC	Office of Classification
OCA	Original Classification Authority
OCRWM	Office of Civilian Radioactive Waste Management
ODFSA	Officially Designated Federal Security Authority

ODSA	Officially Designated Security Authority
OGA	Other Government Agency
OST	Office of Secure Transportation
OUO	Official Use Only
P_E	Protection Effectiveness
PF	Protective Force
RD	Restricted Data
RDD	Radiological Dispersal Device
RED	Radiation Exposure Device
RW	Radioactive Waste
RWT	Radioactive Waste Transportation
(S)	Secret
SAMACS	Security Alarm Monitoring and Control System
SS	Safeguard and Security
SME	Subject Matter Expert
SNM	Special Nuclear Material
STE	Secure Terminal Equipment
TFNI	Transclassified Foreign Nuclear Intelligence
UCNI	Unclassified Controlled Nuclear Information
USEC	United States Enrichment Corporation
USG	United States Government
VA	Vulnerability Assessment
WG	Working Group
WMD	Weapons of Mass Destruction
XML	Extensible Markup Language