(U) DEPARTMENT OF STATE CLASSIFICATION GUIDE (DSCG 05-01)

January 2005, Edition 1

CONFIDENTIAL

Classified by: Under Secretary for Management, Grant Green, Jr.
Reason: 1.4(c), (d)
Declassify On: 01/20/2020

(U) DEPARTMENT OF STATE CLASSIFICATION GUIDE (DSCG)

A GUIDE FOR THE CLASSIFICATION OF DOCUMENTS
UNDER EXECUTIVE ORDER 12958

(U) I. INTRODUCTION AND BACKGROUND

(U) A. Name and Citation

(U) This Guide is entitled *Department of State Classification Guide, 2005, Edition 1.* It is abbreviated DSCG 05-01. The abbreviated title shall be used when citing the Guide in classification actions. The title shall remain unchanged until changes are made to the Guide itself. When changes to the Guide are made, they shall be indicated in the title by the year in which they are made and the number of the change for that year. For instance, the first change to this Guide in 2005 would change the abbreviated title to DSCG 05-02. The second change in 2005 would result in DSCG 05-03.

(U) B. Purpose and Scope

(U) This Classification Guide is for the use of State Department employees in classifying information under the terms of Executive Order 12958 on National Security Information in documents they create or control. It constitutes the classification authority to be cited by persons without original classification authority (OCA) and should be used also by persons with OCA when the Guide properly describes and characterizes the information to be classified. Documents that are classified using this Guide are derivatively classified under its authority. This Guide does not affect the authority and procedures for classifying derivatively from other documents. While this Guide provides the authority for the protection of national security information, it does not replace sound judgment by classifiers as to the need for, level, and duration of classification. Persons approving documents drafted by subordinates who have used this guide to classify information should assume responsibility for assuring that it has been done properly. For purposes of contractor compliance with national-level safeguarding directives, this Guide is a compliance document for State Department contractors.

(U) This Guide aims particularly at the type of information most often classified at foreign service posts abroad and in Department of State domestic offices. While this Guide is specific as to categories of information that may be classified under its authority, the dynamic nature of foreign affairs requires that the described categories be sufficiently general to encompass most situations requiring the protection of information. There may, nonetheless, be information not covered by this guide that requires classification protection. In those cases, the classifier must seek the authority of an OCA to accomplish the necessary classification action.

(U) Supplemental Guidance. Bureaus are welcome and encouraged to supplement this Guide with additional guidance, classified or unclassified, tailored to their specific requirements and geographical or functional responsibilities, and/or covering aspects of E.O. 12958, as amended, or the ISOO Implementing Directive not covered in this Guide. All such supplemental guidance must be cleared with the Office of Information Programs and Services (A/RPS/IPS), which has overall responsibility for classification guides within the Department. A/RPS/IPS will review such guides to ensure that they are consistent with this Guide and will coordinate, as appropriate, with other concerned bureaus or agencies and, as required, obtain the clearance of the Information Security Oversight Office (ISOO), which has government-wide responsibility for implementation of E.O. 12958 and has reviewed this guide. Nothing in this Guide is intended to preclude elaboration of E.O. 12958 and the ISOO Implementing Directive as they apply to the specific requirements and responsibilities of individual bureaus in the Department. Guides in effect at the time of issuance of this Guide remain in effect without amendment. Copies of all such existing guides should be sent to A/RPS/IPS for purposes of establishing and maintaining a central record.

(U) C. Classification Levels

(U) Section 1.2(a) of E.O. 12958 defines the three levels at which information may be classified, as follows:

> *(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.*
> *(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.*
> *(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.*

(U) D. Damage to National Security

(U) The definition of "Damage" is contained in Section 6.1(j) of E.O 12958 and is quoted below. Note that the language specifically equates harm to the foreign relations of the U.S. with damage to the national security:

> *"Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.*

(U) E. Limitations

(U) E.O. 12958, Section 1.7(a), prohibits the classification of information in order to:

1) conceal violations of law, inefficiency, or administrative error;
2) prevent embarrassment to a person, organization or agency;
3) restrain competition; or
4) prevent or delay the release of information that does not require protection in the interest of the national security.

(U) Section 1.7(b) states that "Basic scientific research information not clearly related to the national security shall not be classified."

(U) Section 1.7(c) specifies that information that has been released to the public under proper authority may not be reclassified except under the personal direction of the agency head or deputy agency head (i.e., the Secretary or Deputy Secretary) and then only when it may be reasonably recovered.

(U) Section 1.7(d) specifies that information may not be classified or reclassified after it has been requested either under the Freedom of Information Act, Privacy Act, or the mandatory review provisions of E.O. 12958 except with the personal participation or under the direction of the Secretary, Deputy Secretary or Under Secretary for Management (M). This procedure appears to have been intended to assure the public that classification procedures will not be abused to withhold information from the public that does not truly merit classification protection. M has directed by Notice published in the Federal Register that the authority to take such action be exercised by the Deputy Assistant Secretary for Records Management and Publishing Services (A/RPS). Where classification in these circumstances is required, holders must contact the Office of Information Programs and Services (A/RPS/IPS) to arrange for classification action.

(U) F. Unclassified Protected Information

(U) This Guide concerns only classification of information under E.O. 12958. It does not address how to deal with information that does not meet the criteria for classification on national security or foreign affairs grounds but which may require protection for other reasons. Such information may include, for example, personnel and other privacy protected information, trade secrets and confidential commercial information, deliberative process, attorney work-product and attorney-client information and law enforcement information. Additional categories of such information include critical infrastructure or sensitive homeland security information that is sensitive for security or anti-terrorism reasons. All such information should be treated as Sensitive But Unclassified (SBU) and, when prudent, marked as SBU. Most important, persons handling such information must be aware that SBU is not a security classification and does not protect national security information from unauthorized disclosure. In the case of certain unclassified nuclear information controlled under the Atomic Energy Act, additional markings will be required.

(U) G. Classification Does Not Depend on the Medium:

(U) Classifiers need constantly to bear in mind that if the information is classified it needs protection regardless of the medium in which it is contained. In addition to telegrams and e-mails for example, this would include action or information memoranda, including legal memoranda of opinion, biographic reports, position papers, think-pieces by participants in diplomatic activity, intelligence analyses or unpublished studies by government or outside experts working for the government (e.g. on boundary, water-rights or refugee issues). If classified information is put on a disk, the disk needs to be marked appropriately. It is important that a draft be marked at least with the highest classification of the information it contains, even if other required markings are not added until the document is circulated.

(U) Use of a secure system such as CLASSNET to transmit e-mails or other information, does not provide protection after receipt. If the information is classified, it must be marked as such before being transmitted. If the information is unclassified but otherwise protectable under law, this should also be indicated by marking the material SBU and with additional captions as appropriate. Failure to apply appropriate markings before transmission risks compromise or unauthorized release.

(U) H. Marking and Procedural Requirements

(U) E.O. 12958, Section 1.6, requires that documents be properly marked at the time of classification with (1) the classification level (Confidential, Secret or Top Secret); (2) the identity, by name and position, of the OCA; (3) office of document origin if not otherwise evident from the OCA title; (4) reason for classification; and (5) declassification instructions (i.e., a date or event for declassification.) The creator of a document shall mark each portion to indicate the classification level. When a document is marked with a classification level (e.g., CONFIDENTIAL) but lacks other necessary markings, it shall be considered as classified at that level and the missing markings added as soon as possible. If identical classified information is contained in both marked and unmarked documents, the unmarked document shall be considered to be classified at the level and duration of the marked document and marked appropriately as soon as possible.

(U) For persons using this guide as classification authority, the citation of this guide will take the place of the name and position of the OCA. The authority should be listed as Department of State Classification Guide as abbreviated "DSCG" plus year and edition indicators. This should be followed by the paragraph letter or letters from Part III of this Guide describing the reason(s) for classification; this will constitute the reason for classification. The paragraph letters all correspond to the subsections of Section 1.4. of E.O. 12958. I.e., A corresponds to 1.4(a), military plans, weapons systems, or operations; B corresponds to 1.4(b), foreign government information; D corresponds to1.4(d), foreign relations or activities, etc. "Declassify on" should be followed by an event or a date 25 years or less from date of origin. (There is a single important exception to the 25 year limit described below under Duration.)

(U) Examples.

(U) The marking on the first page of a document classified under authority of this guide because it contains foreign government information being classified for twenty years from January 5, 2005 would read:

Derived from: DSCG 05-1, B
Declassify on: 01/05/20025

(U) A document classified because of foreign relations and economic matters relating to national security for a duration of 25 years from 01/05/05:

Derived from: DSCG 05-1, D,E
Declassify on: 01/05/2030

(U) More detailed marking instructions, as well as other reference materials relating to classification and the FOIA, are available on the Department's ClassNet website. Go to the Department's Homepage (http://intranet.state.sgov.gov), click on FOIA at the top, which will bring up the InfoAccess page, and click on "Classifying Information" in the box to the left. (Similar information is available through the Intranet and Internet.)

(U) I. Duration of Classification

(U) 1. Classifying Up to 25 Years At Origin. The criteria governing the duration of classification at the time information is originally classified have been simplified in Section 1.5 of the March 2003 amendment to E.O. 12958. There is no longer a separate set of criteria for classifying information for more than 10 and up to 25 years (the old Section 1.6). The categories of Section 1.4 may be used to classify information up to 25 years at the time of first classification. There is still, however, a bias in favor of a date or event not greater than 10 years. Section 1.5(d) reads in pertinent part:

> *If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for classification for up to 25 years from the date of the original decision. ... .*

(U) 2. Using an Event. It is sometimes possible and useful to designate an event for automatic declassification. This should only be done, however, when the event is reasonably definite and foreseeable. The event cannot be more than 25 years away. Examples where an event might usefully be used could include:

-- Upon signing of the treaty.
-- After the spring 2006 NATO Ministerial.
-- After the Secretary's scheduled March 2005 presentation at the UNSC.
-- When the minutes of the meeting have been approved and published.

(U) At the time of original classification an indefinite or hypothetical event should not be used for declassification. Examples of such incorrect usage would include:

-- When the issue is no longer sensitive.
-- When any party to the talks divulges their content.
-- When countries X and Y improve relations.

(U) 3. Picking a Date. While a significant amount of State Department information will be adequately protected by assigning a classification duration of ten years or less, that duration of classification could be grossly inadequate for many classes of information. This latter is particularly true for information derived from foreign governments and confidential sources and, as discussed below under several individual categories, it applies to other types of information as well. Often there are multiple considerations in determining the duration of classification. While the information provided by a source may be of lessened sensitivity in ten years, the fact that the source provided the information could be sensitive for as long as the source lives. Similarly, the signing of an agreement generally means that much of the related information loses its sensitivity, but a negotiating history of the agreement describing the diplomatic details and discussions could well remain sensitive for many years. It is therefore incumbent upon the user of this guide, as for OCAs, carefully to consider each duration decision.

(U) 4. Not More Than 25 Years. The categories of information described in this Guide may be classified for up to 25 years -- which experience has shown to be a period more than adequate to protect the vast majority of classified information. E.O. 12958 does not authorize original classification beyond 25 years except to protect confidential human sources or human intelligence sources. Because of the generally great sensitivity of these latter kinds of information, and the possibly fatal consequences of unauthorized release, the Information Security Oversight Office (ISOO) has authorized documents containing such information to be marked as exempt from automatic declassification at the time of creation. This will be indicated by use of "25X1-human" on the declassify on line.

(U) Some information other than human-source-derived will also require classification protection for a period longer than 25 years from date of origin. This extension of classification protection will normally take place as a result of the systematic review conducted pursuant to Section 3.4 of E.O. 12958. This review is generally conducted as the 25-year declassification deadline nears, in sufficient time to ensure that still-sensitive information does not become automatically declassified. The categories of information that may be exempted from automatic declassification at 25 years are enumerated in Section 3.3(b) of E.O. 12958. That section of the Order is reproduced in Part IV at the end of this Guide.

(U) 5. Cite All Categories That Apply. As will be evident in the descriptions of classification categories in Section III of this Guide, multiple categories of Section 1.4 of E.O. 12958 may apply to a single document. For instance, information passed by a

foreign government in the course of negotiations for an agreement on exchange of specific scientific information to be used in protecting facilities against international terrorism could be protected under three, and possibly four, categories, i.e. 1.4(b), 1.4(d), 1.4(e) and possibly 1.4(g). All that are applicable should be cited. This will help ensure the level and type of protection required, as well as help determine disposition in the event of a request for declassification and release of the information. Ultimately, it could help defend continued classification if there is a challenge in court.

(U) II. ORGANIZATION AND USE OF THE GUIDE

(U) The categories of information that may be classified are enumerated in Sections 1.4(a) through (h) of Executive Order 12958. This section of the E.O. is reproduced in its entirety at the beginning of Part III of this Guide. Users should become familiar with it. The remainder of Part III of this Guide is a discussion of the application of these classification categories to information in documents created by Department of State personnel. The subject headings in Part III follow the order of the categories in E.O. 12958 and are followed by the applicable E.O. 12958 categories in brackets, e.g., "Foreign Government Information [1.4(b)]". A large majority of State Department documents are classified under E.O. 12958 Sections 1.4(b) (foreign government information) and 1.4(d) (foreign relations). These categories are discussed in considerable detail in Sections III B and III D respectively. Most other categories of classified information in State-created documents will generally have been originally classified by another agency of the federal government, e.g., military plans by DOD or the military services, intelligence by CIA or other intelligence agency, etc. This is particularly true for INR, which produces many all-source documents drawing on material from other agencies. In these cases, the information is to be given a derivative classification in the State document. In consequence, the discussion of the classification of categories of information usually classified derivatively is shorter in this Guide. Bureaus and offices in the Department that create derivatively classified information in such categories may supplement this guide with their own guide.

(U) Each classification category is described generically, usually followed by illustrative examples. In order to give this guide general applicability and to keep it largely unclassified, the examples are not always specific, nor are they intended to be comprehensive. An effort to include in this Guide every possible contingency would produce an unmanageably cumbersome product that could not serve its purpose and would, moreover, have an unacceptably short shelf life. To repeat a point made earlier, and which is essential to the use of this Guide, it is not intended and cannot substitute for the knowledge, experience and judgment of the classifier (whether an individual using this Guide or an OCA). By way of example, Section III D authorizes classifying reporting of negative material about a country's royal family, if release of the information would harm relations with that country. But clearly, the citizens of some European countries, for instance, have a much more relaxed attitude towards their royals than do the citizens of certain Asian countries. Where the former might be unfazed, the latter

could be offended; criticism could even be a crime under host country law. The classifier is expected to appreciate these kinds of cultural differences and to take them into account.

(U) When the creator of a document who does not have original classification authority believes that State Department information not described in this Guide requires classification protection, he/she should obtain the authority of an OCA to classify it.

(U) Order of Discussion of Classification Categories

(U) III. CLASSIFICATION CATEGORIES

(U) ***Section. 1.4. Classification Categories.***
Information shall not be considered for classification unless it concerns:
(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
(f) United States Government programs for safeguarding nuclear materials or facilities;
(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
(h) weapons of mass destruction.

(U) A. MILITARY PLANS, WEAPONS SYSTEMS, OR OPERATIONS. [1.4(a)]

(U) Information in this category might include: military plans for operations or contingencies, scientific or engineering analyses or descriptions of U.S. weapons systems; weaknesses in the current U.S. defense posture; U.S. national and military command, control and communications systems, and nuclear weapon release authority

and agreements; and any other information likely to weaken U.S. weapons systems. With their extensive involvement in various national and international military organizations and operations, State Department officials create numerous documents containing classified information relating to military plans, weapons systems or operations. Virtually by definition, however, classified information in this category is likely to have originated at DOD or one of the armed services. When this is the case, the document should be classified derivatively based on the original classification reason, level and duration. When a State Department official creates information that has not previously been classified, as for instance, a proposal for military response to a particular threat or action, or an analysis of foreign reaction to U.S. military action, the information should be classified SECRET (though CONFIDENTIAL may in some circumstances be adequate) for at least ten and possibly as long as 25 years. If there is question as to the need for, level or duration of classification, classification action should be taken by an OCA familiar with the subject matter.

(U) B. FOREIGN GOVERNMENT INFORMATION. [1.4(b)]

(U) Foreign Government Information (FGI) is defined in Section 6.1(r) of E.O. 12958 as:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
(3) information received and treated as "foreign government information" under the terms of a predecessor order.

(U) Background. In the 2003 amendment to E.O. 12958 the following language was added to the order: *"1.1(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security."*

(U) Virtually identical language had been in the predecessor executive order (E.O. 12356) but was dropped when E.O. 12958 was first issued in 1995. Because the inherent sensitivity of FGI and the negative impact of its unauthorized release is not always clear from the substance of the information, restoration of this language was considered necessary in order to: a) ensure that classifiers gave proper attention to the possible sensitivity of FGI; and b) to defend against legal challenges to classification of FGI. It has not been State Department practice to classify and withhold FGI in the absence of identifiable harm to the national interest. Therefore, the major practical effect of this change, as far as the State Department is concerned, will be to strengthen the government's position when defending the withholding of FGI in court.

(U) 2. General. As discussed above, observing the confidentiality of the exchange of information between governments is a basic requisite for the successful conduct of diplomacy; trust in the discretion of the other side is often essential to successful negotiations and discussions. The expectation of confidentiality applies equally to exchanges between adversaries and friends. Actions that undermine this trust carry costs which must be weighed. Additionally, foreign governments are the frequent sources of information vital to the formulation and execution of U.S. foreign policies. The continued access to this information will generally depend upon our willingness to protect such information and the foreign government as the source. The same may be true of certain exchanges with officials of international organizations and other confidential international organization material.

(U) Generally the foreign-derived information will itself be sensitive and the need for classification will be clear based upon its substance. This will not always be the case, however, so the classifier must calculate the likely reaction of the source to disclosure even if the information is not by itself sensitive, and weigh the effect of that reaction on U.S. foreign policy and foreign relations, including the willingness of the government or official to share information in the future. Some governments are more protective of their information than are others – including even the fact that they have provided information to the U.S. at all. Some governments insist that their information be protected for a set period of time, such as 25 years. In deciding whether to classify, the classifier may conclude that a predictable negative reaction of the originating country to release of its information is of sufficient magnitude to justify classification even in the absence of self-evident sensitivity of the information itself.

(U) If a foreign government or international organization of governments has itself classified the document at a level which corresponds to the U.S. classification "Confidential" or above, the document should be considered properly classified and given protection at least equivalent to the comparable U.S. classification. A U.S. classification may be assigned, but there is no need to do so if the responsible agency determines that the foreign government markings are adequate to meet the purpose served by U.S. classification markings. [Section 1.6(e)]

(U) Not classifying FGI is not equivalent to approving public release. Certain types of information exchanged with foreign governments (e.g. dealing with protocol, administrative and consular matters) are not normally classified by either government, though both parties may regard them as non-public communications. On the American side, considerations such as storage requirements and the need for host and third country U.S. Government employees to have access are likely to be factored into the decision whether to classify. The fact that FGI is not classified at time of receipt does not mean that it would necessarily be released in response to a Freedom of Information Act or other access request. Under procedures for processing such information requests, a determination would be made at the time of the access request whether foreign relations considerations might require withholding from release and, if necessary, whether the document should be classified at that time under the provisions of Section 1.7(d) of E.O.

12958. Classifiers should not use SBU to protect FGI; as a general rule FGI is either classified or it is public.

(U) 3. Types of FGI Likely to Require Classification. FGI can encompass a broad range of types of information, including:

(U) a. High Level Correspondence. This includes letters, diplomatic notes or memoranda or other reports of telephone or face-to-face conversations involving foreign chiefs of state or government, cabinet-level officials or comparable level figures, e.g., leaders of opposition parties. It should be presumed that this type of information should be classified at least CONFIDENTIAL, though the actual level of classification will depend upon the sensitivity of the contained information and classification normally assigned by the U.S. to this category of information. Information from senior officials shall normally be assigned a classification duration of at least ten years. Some subjects, such as cooperation on matters affecting third countries, or negotiation of secret agreements, would merit original classification for up to 25 years.

(U) b. Foreign Government Documents on Matters of Substance. These include, but are not necessarily limited to foreign government diplomatic notes, aides-memoir, position papers, "non-papers" and USG transcriptions of foreign documents e.g. the telegraphic reporting by a U.S. embassy of the text of a foreign government document. Foreign government documents will frequently bear no classification markings when received. Whether the information should be classified will depend upon the sensitivity of the underlying subject to both governments. As a general rule, such FGI should be classified at the highest level normally assigned to this kind of information by either government and for the same length of time as U.S. documents containing similar information. When there is no comparable U.S. information to provide a guide for duration, the FGI should normally be classified for ten years from date of origin.

(C) c. Information Provided Orally by a Foreign Government or International Organization Official. Information provided to the USG by a foreign government or international organization official in the performance of his duties should generally be accorded the same level of protection as comparable information contained in documents. If an official is merely conveying the official position of his government on a then-current issue in bilateral or multilateral relations which has been made public and is well known, there may be no need to protect the information. The foreign government or official, however, might expect such communications to be treated as confidential. There are a number of instances in which the information will almost invariably require classification protection. These might include:

[redacted] b1 (1.4(d))

(U) Often a purely State Department document will include reference to an intelligence presence in a particular country. This may be in the form of information from or about an intelligence source or simply identification of an intelligence presence. A document containing such information should be classified at least CONFIDENTIAL for a duration of 25 years, or 25X1 if it reveals the identity of a human intelligence source.

(U) Roger Channel messages are controlled by the Assistant Secretary, INR. They are used to report sensitive intelligence matters and have very limited distribution. Roger Channel should normally be classified SECRET for a duration of 25 years, or marked 25X1-human if they reveal the identity of a human intelligence source. (Inclusion of information here on Roger Channel does not constitute authority to initiate messages in this channel. This will normally be done by an OCA.)

(U) Cryptologic materials are generally held by the Department on a temporary basis. Cryptologic materials come under the control of the National Security Agency (NSA) and classification determination will generally have been made by that agency. These might include information on: U.S. cryptologic capabilities and vulnerabilities; foreign cryptologic capabilities and vulnerabilities; cryptoperiod dates; and inventory reports of COMSEC material. When there is question about the classification of possible cryptologic information, it should be given to officials in the Department who regularly deal with such information or sent to NSA for a classification determination. In the interim, it should be marked and treated as TOP SECRET/SCI with a duration of 25 years. If storage is not available at the TS/SCI level, it should be marked and treated in the interim as SECRET.

(U) D. FOREIGN RELATIONS OR FOREIGN ACTIVITIES OF THE UNITED STATES INCLUDING CONFIDENTIAL SOURCES [1.4(d)]

(U) As noted above, and outlined in more detail below, the conduct of foreign affairs takes place in a highly fluid and often rapidly changing environment. What is sensitive in a particular country at a particular time may have greater or less sensitivity six months later and have none whatsoever in another country. We have described below the most likely circumstances in which information should be classified to avoid damage to U.S. foreign relations or U.S. diplomatic activity. These should cover, at least by logical extension, most circumstances where information will require classification. The discussion below focuses on foreign countries, but also applies to international organizations where the same considerations apply.

(U) 1. Sensitive Diplomatic Commentary, Reporting and Analysis.

(U) General Considerations. Reporting on and analysis of the internal affairs or foreign relations of a country is a central function of U.S. foreign service posts and is vital to the formulation and execution of U.S. foreign policy. This reporting should be

unclassified when the subject matter is routine, already in the public domain, or otherwise not sensitive. Drafters will sometimes find it preferable to leave out or separately report sensitive information in order to obtain the broadest useful dissemination of the remaining reported information. However, much reporting and analysis necessarily contains material that, if released, would damage U.S. relations with the government or important elements of a country or otherwise undermine U.S interests and should be classified. This could include:

(U) **a.** Reporting and Analysis about the policies of the government, or a political party, or social or economic group. Sensitive commentary in this category warranting classification can be either favorable or unfavorable. The basic question is whether release of the information would complicate U.S. political activities or impair relations. For example, favorable commentary about the policies of opposition parties or personalities could complicate relations with the government. Even neutral commentary could have a negative impact if it gives the impression that the USG is too deeply involved in the country's affairs. However, neutral commentary about a country's current domestic or foreign affairs is unlikely to be very sensitive and therefore may not require a long duration of classification. Classification at the CONFIDENTIAL level for a duration of ten years or less is likely to be adequate for this type of information. (But see Section III.D 7 below when information is derived from a confidential human source.).

(U) When the commentary is negative, the information is inherently more sensitive and likely to require a higher level and longer duration of classification. This could include any kind of negative commentary, whether based on policies or personalities. Especially sensitive examples of negative commentary might include reports of corruption of individual officials, foreign government agencies or other institutions. The possibility that foreign political, economic, religious and social leaders will survive and rebound from adversity again to become significant players on the political or diplomatic scene should not be underestimated and needs to be taken into account when assigning classification duration. The Bureau of Intelligence and Research (INR) produces a broad range of all-source analyses. Most of these reports are derivatively classified from sensitive sources. Where INR reporting is based upon State or unclassified sources, classification will be determined by this Guide or other approved guides (see I.B. Supplemental Guidance). See also Section C on Intelligence Activities.

(C)

1.4d

[redacted]

(C) **c.** Biographic Information. Biographic information about foreign persons may be classified or unclassified depending upon content and source of the information as described elsewhere in this guide. When deciding upon the classification of biographic information in State reporting [redacted] writers should take into account local sensitivities such as the deference extended to religious or royal personages or the privacy accorded to female family members.

1.4 (c)(d)

(C) **2. Sensitive Policy Discussions/Recommendations/Plans.**

(C) a. Policy Formulation. The formulation of foreign policy is a broad-ranging and sometimes free-wheeling process in which many options are explored. In addition to critical analytical material, as described above, policy documents may raise policy options in regard to countries, groups or organizations which, if revealed, would damage or impair foreign relations or national security. There are, for instance, situations in which the thoroughness of the policy debate requires consideration of options that should not be made public. [redacted] For instance, knowledge of the fact that the U.S. is exploring adopting a particular posture at the UN or in another international forum could have a possibly broad negative impact. Additionally, policy deliberations need to be protected in order to protect details of the decision process, even for policy options that have been rejected. [redacted]

(U) The level of classification given to policy documents will depend upon the sensitivity of the underlying issues, but a classification of SECRET will often be appropriate. (In rare circumstances where the release of policy deliberations could result in exceptionally grave damage to the national security, a TOP SECRET classification might be appropriate. In these cases, the classification should be derived from an existing TS document, or an OCA with TS authority should be asked to classify the information.) Policy information may also remain sensitive for a considerable period of time. The fact that a particular policy was not adopted or is no longer in effect will not necessarily

diminish the sensitivity of the policy deliberations. Such information should generally be protected for at least ten years; depending on the circumstances, a duration of 25 years could be appropriate.

(U) b. Contingency Plans. The policy process frequently culminates in specific plans for dealing with various actual or potential situations. The same sensitivity described above in relation to the policy debate would probably be embedded in the resulting plan, whether or not it has been implemented, and similar consideration should be given to classifying the information at the SECRET level (and in rare circumstances at the TOP SECRET level) and for a duration of ten or more years. Additionally, references to older contingency plans which remain in effect or which are relevant to current situations or plans should be considered for classification.

(C) 3.

1.4 d

(U) 4. U.S. Involvement in International Disputes

(U) Because of its status as a global great power, there are few international disputes or controversies in which the U.S. does not have an interest, either directly as a party, because a friend or ally is a party, or because of the U.S.'s actual or potential role as mediator or participant in conflict resolution efforts. This includes new controversies but also may include issues which date back many years (or decades) that are still the subject of current negotiations, ongoing dispute, open or hidden resentments, current or potential irredentism, or capable of again becoming contentious issues involving U.S. interests. In those cases where the U.S. has been, or may again be, involved as an intermediary, it is an additional concern that information not be released which would prejudice future negotiations on unresolved issues or impair the U.S.'s ability to continue an intermediary role to resolve those issues. For this reason, it is important that information be classified when its release might cause or revive conflict or controversy, inflame emotions or otherwise prejudice U.S. interests. Classifiers should be aware that

it may be necessary to classify information about newly-arising conflicts, about long-standing ones such as Israel-Palestine and Kashmir, as well as information relating to long-simmering or dormant controversies such the Falklands Islands or Peru-Ecuador.

(U) The potential damage to the national security and foreign relations will, to some extent, be a factor of the U.S. involvement in the basic dispute or settlement efforts. In these cases where there is involvement, a classification of SECRET will frequently be appropriate. As the foregoing discussion suggests, this type of information can remain sensitive for an appreciable length of time, even well beyond the time that the dispute is supposedly "settled". It should, therefore, normally be classified for at least ten and up to 25 years. (During systematic review, this category of information is often exempted from automatic declassification at 25 years.)

(U) 5. Confidential Diplomatic Exchanges and Negotiating Agreements.

(U) In many negotiations and other diplomatic exchanges, particularly but not solely in a bilateral context, it is a deeply rooted and long-standing tradition of diplomatic intercourse that the details of the exchanges between the parties, including commentary, will not be divulged during the course of the negotiations. Most countries expect that their diplomatic communications will be treated with confidence even after the matter under consideration is concluded. As a general rule, therefore, when negotiations or other diplomatic exchanges are conducted in a non-public, off the record, channel, details should be classified. This rule applies to negotiations and exchanges with international organizations as well as with foreign governments. Information obtained from (and in some contexts, shared with) other governments or international organizations of governments in a non-public, confidential exchange should be treated as Foreign Government Information (FGI) and classified for as long as necessary, taking into account both the inherent sensitivity of the information and the expectations of that party. (See section on FGI above.)

(U) In many cases, U.S.-origin classified information relating to the U.S. position in negotiations needs to be classified only until the negotiations have been completed. However, if the same or similar issues are to be separately negotiated with another party or parties, or if an agreement is controversial and is likely to remain a sensitive topic in the public discourse of the other negotiating party, U.S. interests may require longer-term classification of information regarding the negotiations. Additionally, references to prior international agreements that remain classified should generally be classified also.

(U) The sensitivity of the subject matter of a negotiation will dictate both the level and duration of classification. For instance, agreements on defense-related subjects such as mutual defense or force basing agreements are likely to have greater sensitivity than economic or consular agreements. Additionally, agreements on defense subjects may include provisions specifying the classification protection to be given to the negotiating record or the text of the agreement. When this is the case, those terms shall govern classification.

(U) While there is wide agreement that successful negotiations require and justify the classification and withholding of information, there is also a strong belief that citizens have the right to be informed of the commitments the government makes on their behalf. Therefore, information on the negotiation of international agreements ought to remain classified only as long as necessary to protect U.S. interests evident at the time of the agreement. In most cases, this will mean that a duration of ten years or less should be applied unless the particular circumstances, including the terms of the agreement, require a longer duration of classification.

(U) **6. Confidential Relations with Foreign Domestic Entities.**

(C) Various elements of embassies, consulates, or missions abroad will often establish relationships with governmental or non-governmental entities in the host country in order to facilitate their work.

1.4d

(U) Information relating to the security and protection of U.S. individuals and facilities may also be classified under Section 1.4(g). Information relating to security that does not warrant classification may nonetheless require protection and should be treated and marked as SBU. (See Section III.G. below). Information relating to law enforcement investigative materials that does not qualify for classification protection under E.O. 12958 may, nonetheless, be properly withheld from public access under the FOIA and should be labeled SBU.

(U) 7. Confidential Human Sources

(U) A confidential human source is any individual who has provided, or who may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information, or the relationship, or both, are to be held in confidence. (This is distinct from a Human Intelligence Source covered by Section 1.4(c). See III.C. above.) The understanding that there is to be confidentiality need not – and in fact generally will not—be explicit. It is enough that an individual under the circumstances would reasonably anticipate that his U.S. interlocutor would treat the information or the relationship as confidential. The identity of the individual and the information should not be classified in the absence of the threshold of identifiable damage to the national security, but this determination need not focus on the specific individual or information at hand if just divulging the source would be likely to damage confidence in the willingness of the U.S. to protect sources of information passed in the expectation of confidentiality.

(C)

1.4d

(U) Classification at the CONFIDENTIAL level will generally be adequate to protect information identifying a confidential source. However, when the information being provided by the source is itself very sensitive and valuable to the U.S. or if revealing the identity of the source could result in danger to his own or to his family's life, physical well-being or livelihood, a SECRET classification would be appropriate.

(U) Special attention needs to be paid to the duration of classification of information that would reveal the identity of a confidential human source, including

consideration of the possibility of negative action against the source. The duration of classification should be sufficiently long to protect the source from the danger of retribution for as long as he is alive, and longer if there is danger of retribution against his family. While a classification duration of 25 years, or even less, may be adequate in most cases, the Information Security Oversight Office has recognized the continuing sensitivity of source-revealing information and has authorized exempting from 25-year automatic declassification, at time of origin, information that would reveal a confidential human source or human intelligence source. (These are the only categories of information that may be so exempted at time of original classification.) When the classifier determines that a confidential human source may require protection for longer than 25 years, he shall make the entry "25X1-human" on the duration line. No other date is required and the information shall remain classified until declassified under proper authority.

(U) E. SCIENTIFIC, TECHNOLOGICAL, OR ECONOMIC MATTERS. [1.4(e), 1.4(d)]

(U) Section 1.4(e) authorizes classification of "scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism." State Department personnel will often create documents containing scientific or technical information requiring classification but that information will generally already have been classified elsewhere. A document creator in these cases should derivatively apply the appropriate classification level and duration from the source documents or, if no example is available, seek a knowledgeable OCA to classify the information.

(U) While economic information may similarly have been classified elsewhere and therefore handled as derivative, officials in the Department or abroad will more often make original compilations or analyses of economic matters that require classification. This could include, for instance, analyses of foreign economies or economic sectors, or of the activities of U.S. firms in foreign countries, the release of which would harm economic relations with the country or relatively disadvantage aspects of the U.S. economy. Information classified under this category might, in many instances, also be classified under 1.4(d) as relating to the foreign relations or foreign activities of the U.S. For instance, information or analysis compiled or prepared in connection with the negotiation of an international economic agreement could be classified under both 1.4(d) and (e) if release would harm the U.S. negotiating position. In some cases merely revealing the extent and depth of USG knowledge of aspects of a foreign economy could be harmful to U.S. foreign and economic relations. As noted above, if more than one category of Section 1.4 applies to the same information, all applicable categories should be cited. Generally classification at the CONFIDENTIAL level will provide adequate protection to economic information, but if the information appears to be of particular sensitivity, inherently or because of the context, it should be classified SECRET. Economic information will frequently lose its sensitivity after a particular event such as the conclusion of a negotiation, the signing of a contract or the end of a harvest season. If

the event is sufficiently definite and identifiable, it should be used for classification duration. Economic information will not generally require classification beyond 10 years (but keep in mind the long term need to protect confidential human sources of information).

(U) Classification category 1.4(e) was modified by the 2003 amendment to E.O. 12958 to include the words "which includes defense against transnational terrorism." This language did not arise in the interagency discussions which preceded the issuance of the amendment, so its precise meaning is not clear. On its face, however, the inclusion of this language would appear to authorize classifying scientific, technical or economic information, including U.S.-origin information, that might individually, or in the aggregate, be of use to potential planners or perpetrators of terrorist acts. Thus, information such as that relating to the weaknesses of certain structural designs or the combustibility of certain materials would appear to be classifiable in those circumstances in which there is a likelihood that release would aid terrorism. Absent an identifiable and imminent terrorism connection, a classification of CONFIDENTIAL would normally be adequate as would a duration of ten years. It should be borne in mind that the inclusion of classified information in a document imposes certain storage, transportation and other safeguarding requirements. It should also be recalled that Section 1.7(b) of E.O. 12958, as amended, states that "Basic scientific research information not clearly related to the national security shall not be classified."

(U) F. USG PROGRAMS FOR SAFEGUARDING NUCLEAR MATERIALS OR FACILITIES [1.4(f)]

(U) The Department of Energy (DOE) is responsible for U.S. Government programs for safeguarding nuclear facilities or materials within the U.S. Department of State officials incorporating such information in Department of State documents should classify the material derivatively based on a referenced document or DOE guidance. Persons who lack a DOE guide but believe that information requires classification under this category should either obtain the assistance of a Department of State OCA knowledgeable in the subject area, or send the material without delay to the Department of Energy for a classification determination. The material should be marked as SECRET for purposes of transmission and all copies should be protected at that level pending a DOE determination.

(U) Department officials occasionally create documents containing information about the safeguarding and vulnerabilities of foreign nuclear facilities and materials or nuclear materials in international transit. Frequently the information will have been originally classified by DOE or another agency or will be covered by a DOE or other agency guide. In those cases, the information should be derivatively classified at the appropriate level. Department of State originated information about safeguarding foreign nuclear facilities or materials should normally be classified SECRET for a duration of at least 10 and up to 25 years depending on the best estimate of how long the information is likely to remain relevant to U.S. security concerns. When written guidance is not

available, it is preferable that such information be classified by an OCA familiar with the subject matter. [redacted]

(U) G. VULNERABILITIES OF SYSTEMS, INSTALLATIONS AND PLANS [1.4(g)]

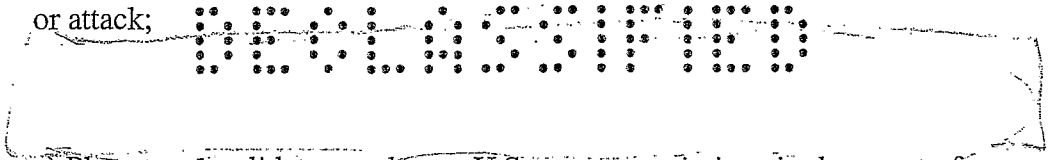
(U) Section 1.4(g) authorizes classification of information that concerns "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, which includes defense against transnational terrorism." The underlining above indicates the language that was added in the March 2003 amendment to the Order. While the additions were arguably covered by the previous language, their addition reflects the post 9/11 concern that the classification system be capable of adequately protecting all information concerning vulnerabilities or capabilities the release of which could compromise U.S. security.

(U) Department-originated information relating to installations and infrastructures should be protected from unauthorized release to the general public if it could be useful to individuals or organizations that might harm U.S. facilities or installations. Much of that information, however, does not require assignment of a security classification and may be designated and marked as SBU. Other information will, because of its greater sensitivity and possible use to individuals and groups hostile to U.S. interests, require classification under this section. With over two hundred embassies, consulates and missions abroad, the Department has particular vulnerability and responsibility in regard to this category of information. Attacks on U.S. facilities and personnel in Africa, the Middle East and elsewhere underline the importance of protecting this category of information. As regards information relating specifically to the design and construction of overseas facilities, the Bureau of Diplomatic Security has issued a detailed guide entitled Security Classification Guide for Design and Construction of Overseas, Facilities – May 2003. It is available from the Bureau of Diplomatic Security or through Regional Security Officers at post. Nothing in this Guide is intended to amend or change that guidance.

(C) When classifying, classifiers must balance the degree of protection given to the information with the reality that achieving a secure environment will sometimes require sharing information with non-cleared persons, e.g., local officials, facilities maintenance personnel, and local security guards. Below is a non-inclusive, illustrative list of categories of information that may require classification protection in whole or in part:

a) The emergency and evacuation plans of embassies and missions abroad;
b) information on structure, design and layout of current USG facilities;
c) details about security and anti-sabotage, anti-terrorism equipment or techniques that might be useful to planning an attack on U.S. persons or facilities [redacted] 1.4(g)

d) methods of protecting U.S. persons and facilities against physical penetration or attack;



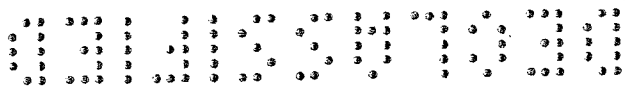
g) Plans to consolidate or relocate U.S. overseas missions in the event of a national emergency.
h) details of negotiations or arrangements with foreign governments to coordinate anti-terrorism actions and practices.

(U) While classification offers the best protection, these kinds of information often need to be shared with uncleared Americans or foreign persons and classification, therefore, may not be appropriate. While not within the scope of this Guide, such information may be properly designated as SBU, bearing in mind that SBU is not a classification. Where classification is warranted, classification at the CONFIDENTIAL level will often be adequate and most appropriate, especially when the information needs to be widely shared, particularly with other agencies where personnel clearances at the CONFIDENTIAL level are the norm. When the sensitivity of this type of information requires, it should be classified at the SECRET level. When classified, information in these categories should normally be classified for as long as the information is likely to remain current and sensitive, usually at least 10 years, but not generally for as long as 25 years.

(U) Frequently Department officials will incorporate another agency's information relating to these categories into Department of State documents; for instance, Secret Service information in a message on presidential travel. When this is the case, the information should be classified derivatively, based upon the other agency's classification level and duration unless the Department of State information in the document requires a greater level and duration of protection, in which case it shall be classified based upon this Guide or an OCA decision.

(U) H. WEAPONS OF MASS DESTRUCTION (WMD). [1.4(h)]

(U) Section 6.1(pp) of E.O. 12958 reads: "Weapons of mass destruction' means chemical, biological, radiological, and nuclear weapons." Information should be classified under this category to protect against proliferation of these weapons and to help prevent terrorist groups or other potential adversaries from either acquiring these weapons or the technical information that could be used to develop these weapons. Additionally, information that would assist a potential developer of weapons of mass destruction in evading monitoring and detection by the United States and its allies and international verification bodies such as the International Atomic Energy Agency or the Organization for Prohibition of Chemical Weapons should be considered as assisting in the development of such weapons and be classified accordingly.



(U) 1. Chemical and Biological Weapons (CBW). Information that would assist in the acquisition, development, design, and manufacture of CBW systems and delivery systems and the development of homemade CBW systems that could be used by terrorists is likely to have been developed and originally classified by another agency. State classifiers should derivatively apply the original classification level and duration. In the event that a Department official creates a document containing such information for which there is no indication of previous classification, it should be classified CONFIDENTIAL or SECRET depending upon the classifier's best estimate of the sensitivity of the information, with a classification duration of at least 10 years.

(U) 2. Radiological Weapons. Information that would assist in the acquisition, development, design, and manufacture of a radiological weapon and its delivery systems and the development of homemade radiological weapons that could be used by terrorists is likely to have been developed and originally classified by another agency. State classifiers should derivatively apply the original classification level and duration. In the event that a Department official creates a document containing such information for which there is no indication of previous classification, it should be classified CONFIDENTIAL or SECRET depending upon the classifiers best estimate of the sensitivity of the information, with a classification duration of at least 10 years. In addition, since radiological weapons contain nuclear material, some information related to radiological weapons could be classified as nuclear weapons information discussed below.

(U) 3. Nuclear Weapons. U.S. nuclear weapons information falls under the authority of the Department of Energy (DOE) under the terms of the Atomic Energy Act of 1954 (AEA). DOE classified information falls into three categories: a) National Security Information (NSI) which is classified under the authority of the present and previous executive orders, such as E.O. 12958; b) Restricted Data (RD); and c) Formerly Restricted Data (FRD). The latter two classification classes are authorized by the AEA, and are administered by DOE. RD concerns the design, manufacture or utilization of atomic weapons, the production of special nuclear material (e.g., plutonium and uranium 235), and the use of special nuclear material in the production of energy. RD is controlled by DOE alone. FRD applies to information that has been removed from the RD category after DOE and DOD have determined it relates primarily to the military use of atomic weapons and can be adequately protected as NSI. Examples of FRD include information about nuclear weapons stockpile quantities, safety and storage, and deployment -- foreign and domestic, past and present. DOE shares control of FRD with DOD.

(U) a. NSI should be considered for classification under Section 1.4(h) if it:
(1) could reasonably be expected to assist other nations or terrorists in acquiring, designing, building, testing, or deploying a nuclear weapon, including component parts or nuclear material;
(2) is identifiably intelligence on foreign nuclear weapons;

(3) would assist a foreign nation or terrorists to circumvent U.S. and allied systems or international safeguards and verification measures for the detection of CBW and nuclear weapons.

(U) b. RD and FRD. Department officials do not have the authority to classify information as RD under the Atomic Energy Act. Information identified as RD should be sent to DOE for classification. In the interim, it should be handled as NSI SECRET. Information that is FRD should be marked as FRD and be given an NSI classification of SECRET with a classification duration of 25 years. Some records containing FRD information have previously been released to the public. The fact that the same or similar information has been previously released does not mean that the FRD should not now be classified. Nothing in E.O. 12958 supersedes any requirement of the AEA with regard to classification.

(U) IV. EXEMPTION FROM AUTOMATIC DECLASSIFICATION AT 25 YEARS

(U) E.O. 12958 does not permit classification of information at time of creation beyond 25 years except in the case of information that would reveal the identity of a confidential human source or human intelligence source. It does, however make provision for the subsequent exemption from automatic declassification at 25 years of information that must be protected to prevent damage to the national security. Though this exemption may be done at any time after 20 years from date of classification, it will normally take place during systematic review prior to transfer the National Archives for permanent safekeeping.

(U) The categories of information that may be exempted at 25 years are defined in E.O. 12958 Section 3.3(b):

> ***Sec. 3.3. Automatic Declassification.***
> *(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:*
>
> > *(1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;*
> >
> > *(2) reveal information that would assist in the development or use of weapons of mass destruction;*
> >
> > *(3) reveal information that would impair U.S. cryptologic systems or activities;*

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

(9) violate a statute, treaty, or international agreement.