



governmentattic.org

"Rummaging in the government's attic"

Description of document: Department of State Declassification Guide 2019

Requested date: 31-March-2020

Release date: 24-October-2024

Posted date: 04-November-2024

Source of document: Freedom of Information Act Request
U. S. Department of State
Office of Information Access Liaison, A/SKS/IAP/IAL
2201 C Street N.W., Suite B266
Washington, D.C. 20520-0000
Fax: (202) 485-1669
[Electronic Request Submission](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



United States Department of State

Washington, D.C. 20520

October 24, 2024

F-2020-05113

This letter responds to your March 31, 2020, request submitted to the Department of State (“the Department”), pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, in which you requested *copy of the State Department Declassification Guide, approved by ISCAP on December 3, 2018*. The Office of Information Programs and Services received your FOIA request on April 1, 2020, and assigned it tracking number F-2020-05113. Please include the tracking number in all future communications concerning this FOIA request.

The Department conducted a search for information responsive to your request and located the enclosed record. Where applicable, we have considered the foreseeable harm standard when reviewing this information and applying FOIA exemptions. As such, we have determined that some information is exempt from release pursuant to the following FOIA exemptions:

- 5 U.S.C. § 552(b)(6), which concerns material that, if released, would constitute a clearly unwarranted invasion of an individual’s personal privacy, and
- 5 U.S.C. § 552(b)(1), which protects information that is properly classified in the interest of national security pursuant to Executive Order 13526.

This action closes your request in this office. For further assistance or to discuss any aspect of your request, you may contact our FOIA Requester Service Center or our FOIA Public Liaison at FOIAStatus@state.gov or by telephone at (202) 261-8484. Please include the DOS case number in all communications concerning this FOIA request.

If you are not satisfied with the Department's determination in response to your request, you may administratively appeal by writing to: Appeals Officer, Office of Information Programs and Services, U.S. Department of State, A/GIS/IPS, HST Room B266, 2201 C Street, NW, Washington, D.C. 20520, by emailing to FOIAAppeals@state.gov, or by faxing to (202) 485-1718. Appeals must be electronically submitted or postmarked within 90 calendar days and include a copy of this letter, clearly stating why you disagree with the determination set forth in this response.

Finally, if you are not satisfied with the Department's determination in response to your appeal you may contact the Office of Government Information Services at the National Archives and Records Administration to inquire about the FOIA Mediation Services they offer. The contact information is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, email address: ogis@nara.gov; telephone: (202) 741-5770; toll free number: 1-877-684-6448.

Sincerely,

**JAMES A
ROSENBAUM**

Digitally signed by
JAMES A ROSENBAUM
Date: 2024.10.24
07:45:27 -04'00'

James A. Rosenbaum
Branch Chief
Statutory Compliance and Research Division
Office of Information Programs and Services

Enclosures: As stated

~~SECRET~~

Declassified in Part

(b)(6)

Senior Reviewer
US Department of State
December 18, 2023



**DEPARTMENT OF STATE
DECLASSIFICATION GUIDE
FOR**

**EXEMPTION FROM AUTOMATIC DECLASSIFICATION
AT 25 YEARS UNDER SECTION 3.3(b) of E.O. 13526,
&
EXEMPTION FROM AUTOMATIC DECLASSIFICATION
AT 50 YEARS UNDER SECTION 3.3(h) of E.O. 13526
DECEMBER 3, 2018**

**Approved by the Interagency Security Classification Appeals Panel
on January 31, 2019**

Derived From: DSCG 17-1, C, D
Declassify on: Dec 31, 2043

~~SECRET~~

DECLASSIFIED IN PART

(U)TABLE OF CONTENTS
(U)GUIDE FOR THE EXEMPTION FROM AUTOMATIC & SYSTEMATIC
DECLASSIFICATION OF RECORDS UNDER PART 3 OF EXECUTIVE ORDER 13526
of December 29, 2009

- I. (U) INTRODUCTION AND BACKGROUND 1
 - A. (U) PURPOSE AND SCOPE 1
 - B. (U) CONTEXT OF E.O. 13526 2
 - C. (U) RELATION TO THE FREEDOM OF INFORMATION AND PRIVACY ACTS 2
 - D. (U) FILE SERIES EXEMPTIONS 3
 - E. (U) REFERRALS 3
 - F. (U) INCORPORATION 3
 - G. (U) PROCEDURAL REQUIREMENTS 3
 - 1. (U) Mandatory Declassification Reviews and Freedom of Information Act Reviews 3
 - 2. (U) Marking 3
 - 3. (U) Age Appropriate Exemptions 4
 - 4. (U) Using a Declassification Event 4
 - H. (U) COMPROMISED INFORMATION 4
- II. (U) ORGANIZATION AND USE OF THE GUIDE 6
- III. (U) EXEMPTION FROM DECLASSIFICATION AT 25 YEARS 7
 - A. (U) INTELLIGENCE MATTERS 7
 - 1. (U) Confidential Source or Human Intelligence Source 7
 - 2. ~~(S)~~ Human Intelligence Source or Intelligence Method or Relationship 8
 - 3. (U) Roger Channel 9
 - B. (U) WEAPONS OF MASS DESTRUCTION 9
 - 1. (U) Nuclear Weapons 10
 - C. (U) CRYPTOLOGIC INFORMATION 12
 - D. (U) U.S. WEAPONS SYSTEM TECHNOLOGY 12
 - E. (U) U.S. MILITARY WAR PLANS 12
 - F. (U) DIPLOMATIC RELATIONS 13
 - 1. (U) Foreign Government Information 13
 - 2. (U) Sensitive Diplomatic Commentary, Reporting, and Analysis 18
 - 3. (U) Sensitive Policy Discussions/Recommendations/Plans 20
 - 4. ~~(C)~~ (b)(1); 1.4 (d)] 20
 - 5. (U) Confidential Negotiations & Agreements 21
 - 6. ~~(C)~~ (b)(1); 1.4 (d)] 22
 - G. (U) PROTECTION OF THE PRESIDENT AND OTHER OFFICIALS 22
 - H. (U) EMERGENCY PREPAREDNESS & VULNERABILITIES OF INSTALLATIONS AND INFRASTRUCTURE (U) 23
- I. (U) STATUTES, TREATIES, & INTERNATIONAL AGREEMENTS 24
- IV. (U) FURTHER EXEMPTION FROM AUTOMATIC DECLASSIFICATION AT 50 YEARS 26
 - A. (U) CONFIDENTIAL HUMAN SOURCES 50x1-HUM 26
 - B. (U) DIPLOMATIC RELATIONS 50X6 27
 - 1. (U) Nuclear Policy Options and Contingency Planning for Major Warfare 27
 - 2. (U) Strategic Information of Continuing Critical Importance to an Ally 27
 - 3. International Agreements Protected Past 50 Years (U) 28
 - 4. (U) Information That Would Cause Serious Harm to U.S. Relations with a Foreign Government 28
 - 5. (U) Weapons of Mass Destruction 29
 - C. (U) STATUTES, TREATIES, & INTERNATIONAL AGREEMENTS 50X9 29

This page was intentionally left blank.

**(U) GUIDE FOR EXEMPTION FROM AUTOMATIC & SYSTEMATIC
DECLASSIFICATION OF RECORDS
UNDER SECTION 3.3 OF EXECUTIVE ORDER 13526 of December 29, 2009**

I. (U) INTRODUCTION AND BACKGROUND

A. (U) PURPOSE AND SCOPE

(U) This Guide is for the use of trained State Department reviewers of classified material in determining whether information of permanent historical value should be exempted from declassification for an extended period. It is based on the premise that all information contained in State Department records older than 25 years should be declassified unless that information is properly identified and exempted from declassification in accordance with one or more of the nine categories listed in Section 3.3(b) or Section 3.3(h)(2) of Executive Order (E.O.) 13526.

(U) Users of this Guide should use their professional experience when reviewing classified national security information for declassification and conduct the appropriate research to prevent the continued withholding of information that should be released. This research should take into account information previously released by the U.S. Government, including information previously declassified by the Interagency Security Classification Appeals Panel (ISCAP):
<https://www.archives.gov/declassification/iscap/decision-table>.

(U) Only information detailed in the specific exemption elements in this Guide are authorized to be exempted from declassification at 25 years or later. All other information should be declassified unless the information may be exempted by another agency, or is Restricted Data or Formerly Restricted Data.

(U) If the information falls into those categories, it must be referred for review by those with the authority to make that determination in accordance with section 3.3(d)(3) of E.O. 13526. Instructions on what information may be referred are contained in this Guide.

(U) Before referring information to another government agency, confirm the agency has not waived their equity and is eligible to exempt information as identified in the most recent Information Security Oversight Office (ISOO) Notice that provides guidance on Agencies eligible to received referrals, available on www.archives.gov/isoo/notices.

(U) If information is not the equity of another agency, and its release does not cause damage to national security, it should be declassified. Other statues or restrictions may apply before the information may be publicly released.

(U) This Guide may be used by other agencies to identify equities of interest to State. In the absence of a specific interagency agreement, other agencies should send to the State Department for review any State equities "that could reasonably be expected to fall under one or more of the exemptions in section 3.3(b) of the Order."

(U) In accordance with Section 3.7(c)(1) of E.O. 13526, this Guide, or detailed declassification guidance, will be provided to the Director of the National Declassification Center at the National Archives and Records Administration.

B. (U) CONTEXT OF E.O. 13526

(U) E.O. 13526 supersedes E.O. 12958, as amended, which was first issued by President Clinton in April 1995 and amended by President Bush in 2003. This Order mandates the automatic declassification of 25-year old national security information in records of permanent historical value unless they had been reviewed and determined to qualify for exemption from automatic declassification under criteria defined in the Order. Classified records thus become automatically declassified on December 31 of the year that is 25 years from the date of origin unless their classification is extended according to such criteria.

(U) This Guide implements the criteria for exemptions and review in EO 13526 signed by President Obama on December 29, 2009.

C. (U) RELATION TO THE FREEDOM OF INFORMATION AND PRIVACY ACTS

(U) Material that no longer merits protection under the terms of E.O. 13526 may, nonetheless, not be releasable to the public under the terms of other provisions of law. Section 6.2(d) of E.O. 13526 is specific in this regard: "Nothing in this Order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended."

(U) The Atomic Energy Act of 1954, as amended, preempts E.O. 13526 with respect to certain nuclear and atomic information. See Section II.B.3 below.

(U) Time will have eroded the applicability of FOIA exemptions in many cases, in particular, the (b)(2) internal personnel practices exemption and the (b)(5) deliberative process exemption that protects materials created during the decision making process. The latter may no longer be used after 25 years. There are other types of information, however, that should be withheld under FOIA exemptions, even if it is more than 25 years old. These might include: confidential financial or commercial information [(b)(4)], personal information, the release of which could result in unwarranted invasion of personal privacy [(b)(6)]; and certain law enforcement information [(b)(7)]. Other information may be exempted from public release by separate statutes. These FOIA (b)(3) statutes include, for instance, arms export control records and information concerning the issuance or denial of a visa or permit to enter the United States.

D. (U) FILE SERIES EXEMPTIONS

(U) The Department of State does not have any approved File Series Exemptions (FSEs). The process for FSE approval is in Section 3.3(c) if E.O. 13526.

E. (U) REFERRALS

(U) All referrals to other agencies are to be made in accordance with section 3.3(d)(3) of E.O. 13526. Each of the following conditions must be met: the information must originate with another agency (or affect the interests or activities of that agency with respect to classified information); the information must reasonably be expected to fall into an exemption category; and the agency must be eligible to receive referrals as identified in the appropriate ISOO Notice, available on www.archives.gov/isoo/notices.

F. (U) INCORPORATION

(U) This Guide does not allow the State Department to incorporate exemptions into its classification guidance under Section 2.2(e) or E.O. 13526.

G. (U) PROCEDURAL REQUIREMENTS

1. (U) Mandatory Declassification Reviews and Freedom of Information Act Reviews

(U) Mandatory Declassification Reviews (MDR) on records 25 years or older must also be in accordance with this Guide. Freedom of Information Act (FOIA) reviews of records 25 years or older may apply the FOIA (b)(1) to only information that meets the exemption provisions of this Guide (FOIA exemptions (b)(2) through (b)(9) are in no way governed or addressed by this Guide).

2. (U) Marking

(U) If in 25 year review it is determined that a document qualifies under the exemption criteria of E.O. 13526 and must remain classified for longer than 25 years, it must be tabbed (collared) with the Standard Declassification Review Tab (SF-715). No markings shall be made on the document. The tab should be marked with all appropriate information—including referral information and changes to classification if applicable. Documents being reviewed in electronic form will have the same information as specified on the SF-715, entered as provided in the computer program.

(U) All relevant exemption categories, 3.3(b)(1) through 3.3(b)(9), should be indicated on the SF-715 as 25X1 through 25X9 to indicate withholding beyond 25 years from the date of the document. The Department has only a limited number of approved exemptions to withhold material after 50 years (see below). If a document is to be held beyond 50 years

(see Part III below), use either an approved 50x exemption or refer it to the equity holding agency for appropriate application.

(U) Only 25X exemptions may be applied to records reviewed in anticipation of automatic declassification at 25 years—except for the 50X1-HUM and 50X2-WMD exemptions (see below). Records exempted under 25X will be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin of the record. If information must continue to be withheld, a reviewer must apply an ISCAP approved 50X exemption within 5 years of that automatic declassification date. Records exempted under 50X shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin of the record.

3. (U) Age Appropriate Exemptions

(U) Only 25X, 50X1-HUM, and 50X2-WMD exemptions may be applied to records reviewed in anticipation of automatic declassification at 25 years (i.e., in reviews conducted in 2018, for records dating between 1974 and 1998). Other than 50X1-HUM and 50X2 WMD, 50X exemptions may only be applied to records approaching automatic declassification at 50 years (i.e., in reviews conducted in 2018, for records dating between 1949 and 1973).

(U) Records exempted under 25X shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin of the record, unless an approved 50X exemption is applied within 5 years of the automatic declassification date. Records exempted under 50X shall be automatically declassified on December 31 of the year that is no more than 75 years from the date of origin of the record, unless an approved 75X exemption is later applied within 5 years of the automatic declassification date.

4. (U) Using a Declassification Event

(U) It is sometimes useful to designate an event for automatic declassification, but such an event should be reasonably definite and expected to occur within 25 years. An indefinite or hypothetical event should not be used, e.g., “when the issue is no longer classified,” or “when countries X and Y improve relations.”

H. (U) COMPROMISED INFORMATION

(U) This section provides guidance for determining if historical records pertaining to the compromise of classified information should be declassified.

(U) *Background on Compromised Information*

(U) Compromised information results from the unauthorized disclosure or release of classified information. Compromised information is not automatically declassified because of its unauthorized disclosure (see section 1.1(c) of E.O. 13526). In addition, as described below, information about compromises and follow-on investigations may be

classified if an Original Classification Authority determines it is necessary to limit damage, conceal security system vulnerabilities, and preclude further compromise. In some cases, no attempt is made to retrieve compromised information as such attempts would call attention to the compromise, resulting in greater damage to the national security than if no such efforts were made.

(U) Information released pursuant to an authorized official U.S. Government release is *not* compromised information. When a U.S. Government release occurs, including through any of the following means, a reclassification action following the provisions of section 1.7(c) of E.O. 13526 must be conducted to exempt information.

(U) Official U.S. Government releases include information released in:

- U.S. Government publications;
- U.S. Government websites;
- Testimony in judicial proceedings by U.S. Government officials;
- U.S. Government filings in judicial proceedings;
- Prior authorized declassification actions that have been released to the public; and/or
- Statements by the President, the Vice President, or in official White House releases.

(U) ***Classification of Compromised Information***

(U) As noted above, compromised information is not automatically declassified because of its unauthorized disclosure. In addition, the location of information, formal analysis of its disclosure, and the fact that classified information has appeared in identifiable public documents or has been disclosed during specific presentations, are classified at the same level [CONFIDENTIAL (C), SECRET (S), or TOP SECRET (TS)], category, duration, with any access limitations (e.g. Sensitive Compartmented Information (SCI)) as the compromised information itself. U.S. Government analysis of compromised information may also be classified depending on the information in the analysis.

(U) Information about compromises and follow-on investigations are classified to limit damage, conceal security system vulnerabilities, and preclude further compromise. If revealed, such information assists adversaries by: (a) altering them to the fact of a compromise; (b) providing details that would confirm the value of the compromised information; (c) providing information on vulnerabilities leading to or resulting from the compromise; (d) providing insight into investigative and countermeasure procedures; and/or (e) confirming information that would otherwise remain unclear.

(U) When reviewing information regarding compromises, the information remains classified if (1) the information contained in the documents describing the compromise is sufficient to materially assist an adversary in locating the compromised information, and (2) the additional criteria, described below, is satisfied. Regarding the first requirement, the statement “*The New York Times* in 1965 published classified information” does not

provide such material assistance, as the volume of material is too great to reasonably search without additional "keys." Similarly, the fact that an unspecified document on a specified broad subject contained classified information would also not provide material assistance; however, identification of a specific report number, date, author, etc. probably would.

(U) Second, compromised information or information about investigations of the compromise can only remain classified if all of the following conditions are met:

- 1) There must be an ISCAP approved exemption for the information element that was compromised;
- 2) The information must be within the date range approved for that information element;
- 3) The information must not fall into the categories in section 1.7 of E.O. 13526; and
- 4) The reviewer must be able to describe the damage to the national security caused by the disclosure.

(U) Section 1.7(a) of E.O. 13526 states:

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified 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) If information falls into one of the categories of section 1.7(a), then the information cannot be classified.

(U) In addition, the information must meet the damage criteria established in section 1.1(a)(4) of E.O. 13526, which provides that information may only be classified if its unauthorized disclosure "reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage." Accordingly, if this damage standard is not met, the information must be declassified. *See also* section 3.1(a) of E.O. 13526 ("information shall be declassified as soon as it no longer meets the standards for classification under this Order.")

II. (U) ORGANIZATION AND USE OF THE GUIDE

(U) Part II of the Guide lists the categories of information that may be exempted from automatic declassification at 25 years and up to 50 years as enumerated in Sections 3.3(b)(1) through 3.3(b)(9) of E.O. 13526 and discusses each category from the standpoint of State Department reviewers.

(U) Part III examines limited options for exempting documents from automatic declassification for periods beyond 50 years and up to 75 years as provided in E.O. 13526 Section 3.3(h).

(U) Most State Department documents will have been originally classified because they concern foreign relations, contain information received from a foreign government, reveal the identity of a confidential source, or include information protected by international agreement. Some of the other most frequently encountered categories of classified information in State Department files will have been originally classified by another federal agency such as the Defense Department or an intelligence agency. Unless declassification authority has been delegated to the Department of State, such documents cannot be released until reviewed by the originating agency and/or other equity holders of the information.

(U) The categories below are discussed in broad terms with illustrative examples. An effort to cover the full range of likely classification requirements for every possible contingency would produce an unmanageably cumbersome product which, moreover, would have an unacceptably short shelf life. Situations change.

III. (U) EXEMPTION FROM DECLASSIFICATION AT 25 YEARS

(U) E.O. 13526, Section 3.3(b) "An agency head may exempt from automatic declassification . . . specific information, the release of which should clearly and demonstrably be expected to:"

A. (U) INTELLIGENCE MATTERS

(U) Sec. 3.3(b)(1): 25X1

"Reveal the identity of a confidential human source, human intelligence source, a relationship with an intelligence or security service of a foreign government 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."

1. (U) Confidential Source or Human Intelligence Source

(U) Section 6.1(k) of EO 13526 defines a **confidential source** as "any individual or organization that has provided, or 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." The understanding need not be explicit.

(U) It is critical to note that the type of source is important. Information that is identifiable as human intelligence should be exempted from automatic declassification as 25x1, and, once it reaches the appropriate age, considered for exemption as 50x1 or

50x1-HUM. Information that is identifiable as other types of reporting should be evaluated for potential release.

(U) In State origin material, **confidential source** information is most frequently found in reports of discussions with foreign political, economic, labor, religious, etc., leaders or activists who are speaking frankly about matters of interest to the United States. In most cases, after 25- years, while the information itself may no longer be classified, the source still requires protection.

(U) For example, if an official is simply passing on the views of his government or organization and that information itself is not still classified, continued protection is not be necessary. However, if that person goes beyond his assigned brief to explain candidly why she or he personally thinks the policy of the government was adopted, or provides frank views on its effectiveness, continued protection may be appropriate.

(U) Even if a person is not explicitly named in a text, if the description would allow reasonable identification of the individual from the title or information provided it could require exemption. Often the sensitivity of protecting a source ends with the source's death, but there are a few exceptions. A government or other relationship may need protection beyond the life of a particular individual. There are circumstances where revealing information can lead to retribution to the source's associates, clan or family, or which compromise the willingness of current officials or individuals to share information in confidence with the U.S. Government.

(U) Information that reveals **human intelligence sources** should be referred to the intelligence agency concerned for a determination on continued protection. However, if the substance of the information is itself classified for diplomatic reasons and meets the criteria in section 3.3(b)(6), reviewers should apply the 25X6 exemption at the time of referral.

(U) When protecting a confidential source or human intelligence source it is not required to provide a date or event for declassification. The exemption should be labeled 25X1 and the information would be protected for the full 50 years. Should that same information remain classified past 50 years, see the 50x exemption application below.

2. ~~(S)~~ (b)(1); 1.4 (c)

~~(S)~~ (b)(1); 1.4 (c)

~~(b)(1); 1.4 (c)~~

~~(S)~~ (b)(1); 1.4 (c)
(b)(1); 1.4 (c)

(b)(1); 1.4 (c)

3. (U) Roger Channel

(U) Roger Channel messages are State Department documents controlled by the Assistant Secretary, Bureau of Intelligence and Research (INR). They are used primarily as a privacy channel to and from Chiefs of Mission to discuss sensitive intelligence and law enforcement matters with INR or the Secretary of State, but are also used to convey information and administrative instructions on intelligence matters. Roger Channel is not a Sensitive Compartmented Information (SCI) designator, but rather a specific State communication channel. These messages should not contain SCI material.

(U) Roger Channel documents over 25 years of age may be reviewed normally; those under 25 years require special handling and decaptioning via INR.

B. (U) WEAPONS OF MASS DESTRUCTION

(U) Sec 3.3(b)(2): 25X2

“Reveal information that would assist in the development, production, or use of weapons of mass destruction.”

(U) It is relatively rare for State reviewers to apply this 25X2 exemption to State equities, but information in this category may appear in State records. Additionally, this Guide also provides information for reviewers to use as an aid to equity recognition for referring specific Weapons of Mass Destruction (WMD) information to other U.S. Government agencies. If this information is identified, the documents should be referred to the appropriate agency for review.

(U) Weapons of mass destruction include chemical, biological, radiological, and nuclear weapons. They are defined in 50 U.S.C. 1801(p) as:

- 1) Any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;
- 2) Any weapon that is designed, intended, or has the capacity to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

- 3) Any weapon involving a biological agent, toxin, or vector that is designed, intended, or has the capacity to cause death, illness, or serious bodily injury to a significant number of persons; or
- 4) Any weapon that is designed, intended, or has the capacity to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

(U) Information is classified under this category to protect against proliferation of these weapons and to prevent terrorist groups or other potential adversaries from either acquiring these weapons or the technical information to develop them.

(U) Also included in this category is information that would assist a potential developer of weapons of mass destruction in evading detection and/or monitoring by the U.S. Government—including the Air Force Technical Applications Center (AFTAC) and the Defense Threat Reduction Agency (DTRA)], its allies, as well as international verification bodies (including the International Atomic Energy Agency and the Organization for Prohibition of Chemical Weapons). The inadvertent release of this information could be used to assist in the development of such weapons.

(U) Any information that would assist in the acquisition, development, design, and manufacture of WMD is likely to be encountered in State Department records only as information originated by another agency or an international organization or body. U.S. originated documents should be referred to AFTAC, DTRA, or other appropriate agencies with equity interest in the information. Information provided to the Department by foreign governments or international organizations or agencies should be exempted from automatic declassification using this exemption as well as the 25X1 and 25X6 exemptions.

(U) **Note:** Reporting on the activities of groups believed to be engaged in the acquisition, development, design, and manufacture of WMD systems and delivery systems would not be exempted under this category unless it included technical details of design, manufacture, etc.

1. (U) Nuclear Weapons

(U) Information about nuclear weapons is more likely than other types of WMD to appear in State Department records. Usually, this information is also classified under the provisions of the Atomic Energy Act (AEA), as amended, and administered by the Department of Energy (DOE). Information classified under the AEA, is marked as either "Restricted Data" (RD) or "Formerly Restricted Data" (FRD) and both are excluded from automatic declassification. RD concerns the design, manufacture, utilization, and/or capabilities of atomic weapons, the production of special nuclear material such as plutonium, deuterium, uranium 235, and the use of special nuclear material in the production of energy. RD is controlled by the DOE alone. FRD applies to information that has been removed from the RD category after DOE and the Office of the Secretary of

Defense (OSD) have determined it relates primarily to the military use of atomic weapons. Examples of FRD include information about nuclear weapons stockpile quantities, safety, storage, and deployment—foreign and domestic, past and present. DOE shares control of FRD with OSD. State records are more likely to contain FRD information as this information also concerns foreign storage locations.

(U) If a reviewer detects information which plausibly comes under the AEA, the information must be reviewed by a “trained Historical Records Restricted Data Reviewer.” These are reviewers who have “Q” clearance and have attended and passed the DOE historical records RD reviewer 4-day course. Most State automatic and systematic declassification reviewers are so certified.

(U) National Security Information (NSI) on these subjects should be exempted from declassification for 50 years from date of origin and referred to DOE if release:

- 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;
- Is identifiable intelligence on foreign nuclear weapons;
- Is identified as containing Transclassified Foreign Nuclear Information (TFNI), as defined in 32 CFR 2001.24i3;
- Would assist a foreign nation or terrorists to circumvent U.S. and allied systems or international safeguards and verification measures for the detection of chemical and biological weapons and nuclear tests and weapons.

(U) Restricted Data (RD). A document, or information in a document, that is marked as RD, is excluded from automatic declassification and is controlled by DOE. If, after review under the provisions of the AEA, DOE removes the RD designation of the document, DOE has the responsibility to refer the document to the appropriate agencies for declassification review of any NSI information in the document.

(U) Formerly Restricted Data (FRD). A document, or information in a document, that is marked as FRD is similarly excluded from automatic declassification. DOE and OSD jointly administer control of FRD information and review its control in accordance with 10 CFR 1045. DOE has the responsibility to refer to other agencies any NSI information in the event that DOE and OSD jointly remove the FRD designation from the document.

(U) Unmarked documents which a reviewer determines probably contain RD or FRD information should be referred to DOE as “possible RD,” or “possible FRD”. Such documents may also be exempted and/or referred to other agencies if circumstances warrant. In both instances, records must also be referred to DOE. Documents that, at the time of review, are not marked FRD, but which contain information about specific nuclear weapons storage abroad, clearly also contain State equity that may be protected. They may be exempted for 50 years from document origin under E.O. 13526, sections

3.3(b)(6) and (9). These documents must then be referred to DOE and OSD for determination, as "possible FRD." While some FRD information has been decontrolled by DOE and OSD and the national security information has been officially declassified, some records containing FRD information have been inadvertently been released to the public. This does not preclude their continued classification and withholding under the AEA as determined by DOE and OSD. Nothing in E.O. 13526 supersedes any requirement of the Atomic Energy Act.

C. (U) CRYPTOLOGIC INFORMATION

(U) Sec 3.3(b)(3): 25X3

"Reveal information that would impair U.S. cryptologic systems or activities;"

(U) Cryptologic materials are generally held by the Department on a temporary basis. Cryptologic materials come under the control of the NSA and the original classification will have been assigned by that agency. Documents in this category might include information on: U.S. cryptologic capabilities and vulnerabilities; foreign cryptologic capabilities and vulnerabilities; crypto-period dates; and inventory reports of Communications Security material. All of this information should be referred to the NSA for review. Cryptographic information will usually be found in documents marked as Sensitive Compartmented Information (SCI). If found in non-SCI files, in automatic and systematic review, it should be treated as a "misfiled" document, removed from the box of historical records, and stored in a SCIF until it can be properly transferred to the National Archives SCI depository.

D. (U) U.S. WEAPONS SYSTEM TECHNOLOGY

(U) Sec. 3.3(b)(4): 25X4

"Reveal information that would impair the application of state of the art technology within a U.S. weapons system;"

(U) Documents in this category are rare in State Department files. Information in this category might include: scientific or engineering analyses or descriptions of U.S. weapons systems; technical vulnerabilities of U.S. defense systems; technical details of U.S. national and military command, control, and communications systems, and any other information likely to weaken the effectiveness U.S. weapons systems. In automatic and systematic review, information that appears to fall in this category should be referred to the appropriate Department of Defense entity (usually Army, Navy, or Air Force). If no specific entity can be identified, it should be referred to OSD.

E. (U) U.S. MILITARY WAR PLANS

(U) Sec 3.3(b)(5): 25X5

"Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;"

(U) Information in this category might include: military plans for operations or contingencies; weaknesses in the current U.S. defense posture; nuclear weapon release authority and agreements; and any other information likely to reveal current U.S. military planning. State Department files contain numerous classified documents concerning military operations, some of which were created by the OSD or the armed services, others in the form of Department of State commentaries or analyses of the foreign policy aspects of those plans. Significant information has been previously declassified and published in the *Foreign Relations of the United States* series (FRUS) on U.S. military plans and preparedness in the Cold War era and later. However, prior release of FRD information does not in itself constitute authority for release of this category of information. This information must be referred to the OSD.

(U) State Department records containing or commenting on war plans should be referred to Joint Chiefs of Staff (JCS). Additionally, the National Security Council (NSC) requires referral to the NSC of any records concerning "authorization to use weapons of mass destruction" and/or U.S. policy on "first use of nuclear weapons."

(U) State Department documents that discuss basic national security policy contingencies, as opposed to specific military war plans, should be evaluated under E.O. 13526 category 3.3(b)(6) below, with referral to the NSC and OSD if appropriate.

F. (U) DIPLOMATIC RELATIONS

(U) **Sec. 3.3(b)(6): 25X6**

"Reveal information, including foreign government 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."

(U) For State Department reviewers, this is the most utilized exemption, and the one that requires the most analysis and judgment. It can include almost any aspect of diplomacy with other powers, potentially ranging from criticism of sitting monarchs and politicians, classified foreign government information, diplomatic negotiations, unresolved international issues, sensitive relations with third parties—including members of opposition political parties, journalists, dissidents, Non-Governmental Organizations (NGOs), political exiles, etc.—as well as innumerable other issues.

(U) The conduct of foreign affairs takes place in a highly fluid and often rapidly changing environment. The same issues can remain unresolved or sensitive for decades. Some of the most likely circumstances in which the release of classified information would cause serious harm to relations or diplomatic activity are noted below, but not every case will fit these categories. All judgments should adhere to the "serious harm" criterion as specified in the Executive Order.

1. (U) Foreign Government Information

(U) Foreign Government Information (FGI) is defined in Section 6.1(s) of E.O. 13526 as:

- 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;
- 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
- information received and treated as “foreign government information” under the terms of a predecessor order.

(U) For FGI to qualify for exemption from automatic declassification after 25 years it must satisfy the “serious harm” requirement of E.O. 13526 Section 3.3(b)(6).

Confidentiality of the exchange of information between governments is a basic requisite for the successful conduct of diplomacy. The expectation of confidentiality applies equally to exchanges between adversaries and friends. Actions that undermine this trust carry costs that must be weighed. Among the factors to be considered in evaluating serious harm to the relationship are “the sensitivity, value, utility, and provenance” of the information.

(U) Additionally, foreign governments are the frequent sources of information vital to the formulation and execution of U.S. foreign policies. Continued access to this vital information depends upon our ability to protect such information and the foreign government as the source. The same may be true of certain documents of and exchanges with officials of international organizations.

(U) In reviewing records that contain FGI, it is important to note that some governments are more protective of their information over longer periods of time than are others and that there are specific agreements covering the release of information with certain countries that reviewers should be cognizant of before releasing FGI information—including even the fact that they have provided information to the U.S. Government at all.

(U) All FGI should be evaluated for release or exemption in the light of the originating country’s own policy on the release of its information and whether the release of this information could cause serious harm to U.S. foreign policy interests. Several countries of importance to the United States and NATO have specific rules regarding the release of historical classified information. For example, German and NATO numbered documents are withheld for 30 years, while British documents are eligible for release at 20 years.

(U) All FGI should be evaluated for release and exemption in the light of any international agreements covering the release of certain kinds of information. Reviewers should, as a general rule, not release classified foreign government documents or

significant foreign government information imbedded in U.S. documents until after 25 years (30 for governments with this rule) without the concurrence of the government concerned. This protects the confidence necessary for confidential international discourse. For exempting information beyond 25 years see below.

~~(S)~~ Types of FGI Likely to Require Exemption at 25 years:

- High Level Communications on Matters of Substance. This includes letters, diplomatic notes or memoranda, or reports of telephone or face-to-face conversations involving foreign chiefs of state or government, cabinet-level officials, leaders of opposition parties, and others. This category of information should be evaluated first on the sensitivity of the contained information to both countries as described below and exempted if appropriate. If the information itself is judged not of significant current sensitivity, a declassification date of 25 years from date of origin may still be needed if the source party (or her/his family) is still prominent or in power. If it is determined that release would seriously harm relations with the official or country concerned, a declassification date as long as 50 years from the document date should be applied.
- Foreign Government Documents on Matters of Substance. These include actual foreign government documents as well as U.S. Government transcriptions of foreign documents, e.g., the telegraphic reporting by a U.S. embassy of the text of a foreign government document. Again the decision to exempt should consider the release policy of the foreign government or international organization and the continuing sensitivity of the underlying subject to both governments. Unless the sensitivity of the information dictates a longer period, 25 years from date of origin will normally be an adequate declassification date.

(b)(1); 1.4 (c)

•

(b)(1); 1.4 (d)

•

Examples include:

- Information that is negative or derogatory about a third country's leaders, people, society, politics, or other subject when revealing the information would seriously harm relations between the source's country and the third country;
 - Information about concerted policies or actions of that government and the U.S. Government directed towards another state or states;
 - Information passed in confidence which the other government or official has chosen not to make public and which, even after the passage of 25 years, continues to be classified;
 - Information about internal political or substantive decisions or deliberations which the foreign government or official would not want to become public;
 - Information about cooperation with the U.S. Government in matters of particular local sensitivity that remain sensitive after 25 years. For example, anti-drug and law enforcement efforts tend to have a high degree of long-term sensitivity;
 - Information provided in confidence by a member of an international organization. (Note that the international organization is an "organization of governments." Thus information from the International Committee of the Red Cross (ICRC) is not FGI while information from the United Nations High Commissioner for Refugees (UNHCR) is). Information provided by international non-governmental organizations may be classified, but it is classified using different criteria;
 - Off-the-record candid observations by the official (see Confidential Human Source above).
- In these instances, release of historical information would cause serious harm to U.S. foreign policy interests. While in some instances it might be possible to consult with the foreign government about release, the nature of the FGI in these cases will generally make consultation with the originating government impractical or inappropriate, especially when it is not clear that the information was passed with full authorization of the government. A declassification date 40 years from date of origin generally will provide adequate protection.
 - Foreign Government Information Protected By an International Agreement. The U.S. Government has entered into international agreements and concluded other arrangements with foreign governments that include provisions obligating the U.S. Government to protect from disclosure classified foreign government information that has been provided to it. In particular, the U.S. Government

routinely negotiates and concludes two types of international agreements to ensure the reciprocal protection of classified information exchanged with a foreign government: General Security of Information Agreements (GSOIAs) and General Security of Military Information Agreements (GSOMIAs). GSOIAs and GSOMIAs are framework agreements. While they do not commit either government to share classified information, they commit each government to protect any information that is shared according to the terms of the agreement. While GSOIAs and GSOMIAs contain substantively identical obligations, GSOIAs address the protection of all classified information exchanged between the parties, whereas GSOMIAs address only the protection of classified *military* information that is exchanged. Typically, GSOMIAs are agency-to-agency agreements between DOD and its counterpart, while GSOIAs are government-to-government agreements. Information covered by these agreements must be protected according to their terms, including with respect to obligations relating to the downgrading or declassification of classified information, either of which generally requires the prior written consent of the foreign government. Classified foreign government information that is protected by a GSOIA, GSOMIA, or other specific commitment should be exempted from automatic declassification and may not be declassified unless the reviewer has confirmed by consulting the Red Book that declassification is in accordance with the terms of that agreement, or with the agreement of the relevant foreign government(s). Classified military information should also be evaluated for possible OSD referral before release.

- Additionally, the U.S. Government, as a member of a number of current and former organizations, is bound by agreements governing the handling and release of the documents of those organizations. Information covered by these agreements should be exempted for the period specified under the terms of the agreements under both 25X6 and 25X9 or held for a longer period if the substance requires. Reviewers should use the Red Book for specific guidance.

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

(U) 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 information provides important insight into the factors that have shaped U.S. policy towards a country or region and ought to be released at 25 years. However, in some instances, even after 25 years, certain information will remain sufficiently sensitive to seriously harm U.S. relations with other governments or hinder the pursuit of important U.S. foreign policy interests. Accordingly, such information should be exempted from automatic declassification.

(U) Reporting and Analysis About the Policies of a Foreign Government, Political Party, Social or Economic Group.

- (U) Either favorable or unfavorable commentary in this category could originally have warranted classification, since, for example, favorable commentary about the

policies of opposition parties or personalities could complicate relations with the current government. At 25 years, it is difficult to see how favorable commentary could be sufficiently damaging to warrant continued withholding unless the information also suggested a relationship with the U.S. Government, release of which would seriously harm current U.S. diplomatic activities or impair current diplomatic relations.

- (U) When the commentary is negative, the information is inherently more sensitive. Still, over time, much of this information loses its sensitivity. Examples of negative commentary that may require exemption from automatic declassification might include reports of corruption of individual officials, foreign government agencies or other institutions, if release of the information would seriously harm current diplomatic relations. The possibility that still-living foreign political, economic, religious, and social leaders might still be in power or positions of influence should be taken into account.

(U) Negative or Personal Comments About Individuals and Biographic Reporting.

- (U) When considering the declassification of information about foreign persons, reviewers should take into account local sensitivities such as the deference extended to religious or royal personages or the privacy accorded to female family members of certain countries. Information in State Department documents, including biographic reporting, that is critical of the intelligence, effectiveness, honesty, competence, or other attributes of a foreign person, or information about potentially embarrassing aspects of his or her personal life should be exempted from automatic declassification if the person is still alive and in a position of authority or likely to return to such a position.
- (U) The information should usually not be exempted if the individual is deceased or no longer active and unlikely to return to a position of influence. However, negative information about deceased persons should also be exempted in those more rare situations where release of the information would so offend relatives or other individuals or groups that it would seriously harm foreign relations. When exempting, the declassification date should take into account the length of time the person is likely to remain prominent in the politics or society of the country and, in some cases, the prominence and authority of the subject's family, clan, and political or social group. Information about certain royal families (e.g. the UK) is potentially very sensitive with the capacity to seriously harm relations and should be exempted for up to 50 years or more from the date of the document.
- (U) While there is nothing inherently sensitive about the fact that posts report biographic information, certain aspects of biographic reporting may continue to be sensitive and should be redacted if classified. Classified biographic reports created by other agencies are frequently found in State files. If they reveal the originating agency, they should be referred to that agency for a declassification determination if they are not exempted in their entirety for State equities.

3. (U) Sensitive Policy Discussions/Recommendations/Plans.

(U) Policy Formulation.

- (U) The formulation of foreign policy is a broad-ranging and sometimes unconstrained process in which many options are explored. Usually this information is declassified as it reaches 25-years of age. However, even after 25 years, certain critical analysis documents may propose policy options relating to countries, groups, or organizations which, if revealed, would seriously harm foreign relations.
- (U) There are, for instance, situations in which the thoroughness of the policy debate requires consideration of options that should not be declassified as the options themselves may be sensitive—e.g., the use of military force, concerted diplomatic action, economic sanctions, or other actions that could be viewed as interference in a country's internal affairs.
- (U) The fact that such options had once been considered, even though never implemented, could be considered hostile or demeaning to a country and seriously harm current foreign diplomatic activities, not only in the country most involved, but also in others that consider themselves similarly placed. On the other hand, documents outlining the possibility of such actions against former pariah regimes might be handled more liberally. Keep in mind, policy deliberations may require exemption under section 3.3(b)(6) in order to protect the discussion of options that may be revived in the future.
- (U) Some options are inherently so sensitive—e.g. options involving intelligence operations or the use of force—that classification for 50 years or more from date of origin may be required. In those instances, information should be exempted using Section 3.3(h) of the Order (see below).

(U) Contingency Plans.

- (U) The policy process frequently culminates in specific plans for dealing with various actual or potential situations. The same sensitive issues described above in relation to policy debates may be embedded in resulting plans, whether or not they have been implemented, and similar consideration should be given to maintaining classification. The duration of classification would similarly be dependent upon whether the plan is still in effect.

4. (U) Suggestion of U.S. Involvement in Foreign Domestic Affairs

(U) Most countries are sensitive to indications of U.S. Government influence over their governments, officials, or leaders. This can come in many forms, all of which should be evaluated carefully for release.

(b)(1); 1.4 (d)
(b)(1); 1.4 (d)

(S) In addition to this, Department records contain information relating to most international disputes or controversies. Many such controversies have long been resolved, and the factual and historical information in the records should be declassified. In limited instances, however, conflicts dating from over 25 years ago are still the subject of current negotiations, ongoing dispute, open or hidden resentment, or capable of seriously harming ongoing U.S. foreign relations and activities. It is important that information not be declassified if that information would revive conflict or controversy, inflame emotions, or prejudice the U.S. position if the United States is a party to or mediator in the dispute. Of special concern are those issues in which one or both parties to the controversy is a particularly close friend or ally of the United States and where release of information about the U.S. position or actions would seriously harm current U.S. foreign relations. Reviewers should, again, weigh whether to apply a declassification date of 25 years from date of the document or apply a full 50 years from the document date in the most sensitive cases.

(U) Note: Unless the document is exempted by the State Department, information concerning a covert (i.e., intelligence) role in a country's internal affairs should be referred to the CIA and also to the NSC for declassification determination. Consult the NSC Partial Waiver, which can be found on the ISOO website as Notice 2017-03, for additional guidance when determining what information to refer.

5. (U) Confidential Negotiations & Agreements

(U) U.S.-origin classified information relating to negotiations is eligible for declassification once it reaches 25 years of age. However, any material that was entirely internal to the United States could remain subject to the attorney-client privilege or other applicable Freedom of Information Act exemptions and therefore still not be appropriate for public release.

(U) Moreover, negotiating instructions and fallback positions may remain sensitive after negotiations have concluded. Before releasing negotiation-related material, consult the entries in the Red Book on both negotiation materials and on the relevant subject matter for guidance and to determine if referral to L and / or a Regional Desk is appropriate. Most information on negotiations that remains sensitive should be exempted as 25X6. In instances where information is governed by international agreement and the information

either requires continued classification beyond 25 years or may not be declassified without consent of both parties, it should be exempted as 25X6 and 26X9.

6. ~~(S)~~ Confidential Relations with Foreign Domestic Entities

~~(S)~~ U.S. officials abroad will often establish relationships with both governmental and non-governmental entities in the host country in order to facilitate their work. (This is distinct from intelligence relationships which require referral to CIA or other appropriate intelligence agency.) The continuation and effectiveness of these diplomatic relationships may require that they be kept confidential including, in rare instances, beyond 25 years when declassification would seriously harm ongoing diplomatic activities.

~~(S)~~ Examples can include: cooperation between U.S. consular officials and the local police and immigration authorities on visa matters; security officers' relations with local police on security matters; political officer contacts with minority religious or ethnic groups; political officer contacts with charitable and other NGOs; economic officer contacts with business or labor groups that remain influential, etc. This is not to say that all of these relationships must remain protected at 25 years, but these types of relationships should be carefully evaluated against the serious harm standard before release.

~~(S)~~(b)(1); 1.4 (d)
(b)(1); 1.4 (d)

]

G. (U) PROTECTION OF THE PRESIDENT AND OTHER OFFICIALS

(U) Sec. 3.3(b)(7): 25X7

“Reveal information that would 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 national security, are authorized.”

(U) This category broadly covers information that might facilitate attempts to harm persons authorized for protection, such as the protection given to selected individuals by the U.S. Secret Service, the Department's Bureau of Diplomatic Security (DS), the FBI, the Federal Marshals Service, the security agencies of DOD and the armed services, and the officials of any other department, bureau, or agency of the U.S. government responsible for providing protective services. The protected individuals need not be U.S. citizens. For instance, DS and the Secret Service often provide protective service to selected foreign visitors to the United States. Additionally, this category would apply to information relating to measures taken by DS and other agencies to protect employees

and visitors at the State Department and other U.S. Government facilities in the U.S. and overseas. The kinds of information likely to be encountered include, but are not limited to:

- Details about equipment or techniques that could still be used to protect persons from attack. This might include instruction manuals or standing orders for protective details or security guards, defensive driving techniques, special secure rooms, or weapons and body armor; and
- Emergency contact and evacuation plans for personnel at embassies and other installations abroad that reveal information that could be exploited even after 25 years by terrorists to harm American citizens.

(U) When information described above has been originated by or involves another agency, the information should be referred to that agency. For example, information about Secret Service protection should be referred to Homeland Security for the Secret Service [DHS(USSS)].

(U) Information in this category is often associated with measures to protect systems or installations and facilities, which are covered by Section 3.3(b)(8) of the Executive Order. When this is the case, both exemption categories should be used.

H. (U) EMERGENCY PREPAREDNESS & VULNERABILITIES OF INSTALLATIONS AND INFRASTRUCTURE (U)

(U) Sec. 3.3(b)(8): 25X8

“Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to national security.”

(U) Reviewers should be careful to avoid declassifying information relating to current installations and national security infrastructures that could be used to aid a terrorist. Historically, this information may not have been marked as classified but as LOU (Limited Official Use) or SBU (Sensitive But Unclassified) and would now be considered CUI (Controlled Unclassified Information). When this information is reviewed, reviewers should refer to the State Department’s Classification Guide to determine if this information should be upgraded and marked as classified. If other agency equities are also involved, consider whether the other agency might be asked to upgrade the document.

(U) Use this exemption to protect those overseas emergency and evacuation plans and security surveys which reveal significant continuing Embassy vulnerabilities.

(U) This exemption category includes sensitive Continuity of Government (COG) plans, and the domestic emergency preparedness plans under the jurisdiction of the Department

of Homeland Security or the Department of Defense. If in doubt about the current sensitivity of this type of information, refer it to DHS/FEMA and/or the OSD.

(U) Note: if it is a White House or NSC document, it should also be referred to the NSC as a waiver exception.

I. (U) STATUTES, TREATIES, & INTERNATIONAL AGREEMENTS

(U) Sec. 3.3(b)(9): 25X9

“Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.”

(U) The information described here will generally also be withheld under 25X6 described above. Section 3.3(b)(9) (25X9) is to be used to exempt **classified** information from automatic declassification.

(U) When exempting information under this category, the reviewer must identify the specific section(s) of the statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(U) As described above in section 1 (Foreign Government Information) of the material discussing 25X6, the United States has entered into international agreements and concluded other arrangements with foreign governments that include provisions obligating the U.S. Government to protect from disclosure classified foreign government information that has been provided to it. In particular, the U.S. Government routinely negotiates and concludes two types of framework international agreements to ensure the reciprocal protection of classified information exchanged with a foreign government: General Security of Information Agreements (GSOIAs) and General Security of Military Information Agreements (GSOMIAs).

(U) Information covered by these agreements must be protected according to their terms, including with respect to obligations relating to the downgrading or declassification of classified information, either of which generally requires the prior written consent of the foreign government. Classified foreign government information that is protected by a GSOIA, GSOMIA, or other specific commitment should be exempted from automatic declassification and may not be declassified unless the reviewer has confirmed by consulting the Red Book that declassification is in accordance with the terms of that agreement, or with the agreement of the relevant foreign government(s). Classified military information should also be evaluated for possible OSD referral before release.

(U) The United States, as a member of a number of current and former organizations, is bound by agreements governing the handling and release of the documents of those organizations. Before releasing information on any agreement, see the Red Book for guidance on any release mechanisms associated with that particular agreement, as well as possible referral to L/T and/or the appropriate regional desk.

(U) Provided below is a non-comprehensive sample of agreements that have mechanisms for the review and release of information generated pursuant to them. Before failing any documents from release based on pre-1992 agreements see the list below and consult the Red Book for additional guidance.

- (U) Live Oak. The parties to the Allied quadripartite agreement concerning Berlin contingencies agreed that documents produced by the group could all be declassified by 2005. The exemption of Live Oak documents from automatic declassification should be judged simply on their substance.
- (U) COCOM. Before it was dissolved after the collapse of the Soviet Union, the 17 member countries of COCOM agreed that COCOM documents would be released to the public after 30 years from their date of origin if no member of the former organization interposes objection to release. COCOM documents from U.S. records should be exempted from release for **32 years** from date of origin to allow time for the objection mechanism to be applied.
 - (U) Note: This constraint does not cover U.S. documents relating to COCOM, such as instructions to the U.S. representative.
- (U) North Atlantic Treaty Organization (NATO). NATO has an agreed program of systematic review at 30 years for declassification of most official NATO documents. All unreleased NATO documents, including those reproduced in U.S. records, should be referred to NARA, which maintains the U.S. NATO Registry. U.S. origin documents that report in detail the substance of the meetings of NATO bodies or other classified NATO-origin information should also be referred to NARA for NATO review and, as appropriate, exempted under 25X9 or other 25X categories.
 - (U) Note: NATO information exempted under 25X9 should also be considered for exemption under 25X6 for an appropriate period of years. U.S. position papers and commentary that do not report on official NATO meetings in detail nor contain classified NATO information should be evaluated simply under U.S. guidelines.
 - (U) Much of NATO information has DOD equities and should be evaluated for possible OSD referral.
- (U) Arms control agreements may contain specific prohibitions on release of information concerning their deliberations. For example:
 - - SALT I and ABM Treaty. The SALT I and ABM Treaty Standing Consultative Commission (SCC) regulations both state that their deliberations shall be conducted in private and that the proceedings may not be made public except with the express consent of all Commissioners.

- Note: Considerable information on the SALT I and ABM Treaties has been declassified and is available in the *Foreign Relations of the United States* volume on the topic. Before failing documents on this subject, see history.state.gov/historicaldocuments/frus69-76v32.
- START. Annex I to the Notification Protocol for START spells out in detail the guidelines governing any release of information contained in the notifications under the provisions of the treaty.
 - Note: Considerable information on START has been declassified and is available in the *Foreign Relations of the United States* volume on the topic. Before failing documents on this subject, see history.state.gov/historicaldocuments/frus81-88v11.

(U) If an international agreement specifies a date for declassification or release of the information in question, that date should be used as the automatic declassification date when exempting such information under this section. If the information is protected by a GSOIA, GSOMIA, or other arrangements with a foreign government that obligates the U.S. Government to protect from disclosure classified foreign government information that has been provided to it, such information should be exempted from automatic declassification and may not be declassified without the agreement of the relevant foreign government(s).

IV. (U) FURTHER EXEMPTION FROM AUTOMATIC DECLASSIFICATION AT 50 YEARS

(U) E.O. 13526, Section 3.3(h): “. . . all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

- (1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:
 - (A) the identity of a confidential human source or a human intelligence source; or
 - (B) key design concepts of weapons of mass destruction.
- (2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.”

A. (U) CONFIDENTIAL HUMAN SOURCES 50x1-HUM

(U) Section 3.3(h) provides that, as necessary, a document may be exempted from declassification beyond 50 years and up to 75 years to protect a confidential human source or human intelligence source.

(U) This authority should be used sparingly by State reviewers, since in most cases 50 years will have been sufficient to protect most of our sources as described in Part II.A.1. of this Guide. However, in cases where the individual in question was young at the time of the report and is known to be professionally active, protection beyond 50 years should be considered.

(U) Similarly it should be considered in circumstances where release might bring repercussions upon an individual, family, or organization. Record the exemption as **50X1-HUM**.

(U) Information that reveals human intelligence sources should be referred to the intelligence community element concerned for a decision on protection.

B. (U) DIPLOMATIC RELATIONS 50X6

(U) All of the considerations outlined under Part II.F above for considering exemption from automatic declassification at 25 years are relevant to the review of documents for exemption from declassification at 50 years, except that the criteria for exemption are considerably more stringent. The following contingencies are authorized for exemption beyond 50 years and up to 75 years under **Section 3.3(h)(2)** as "**50X6**."

(U) In making these judgments, reviewers should assess whether the document reveals key, sensitive classified concepts that are still in force or would seriously harm and jeopardize current U.S. diplomatic activities with another nation. The fact that a foreign government would prefer that we hold particular information beyond 50 years is not sufficient grounds to do so unless it is clear that it would "*cause serious harm*" to U.S. foreign relations or ongoing diplomatic activities.

1. (U) Nuclear Policy Options and Contingency Planning for Major Warfare

(U) Whereas specific military plans would always be referred to the OSD, Department of State files contain some high-level proposals and even agreed postures regarding international contingencies that are still relevant and require continued protection. If such documents discuss options still in force, serious contingency actions that could still be invoked, and/or would seriously harm current diplomatic relations if revealed, the documents should continue to be exempted from automatic declassification for an extended period beyond 50 years and up to 75 years from the document date. This should be confined to documents that revealed, or commented in a revealing manner on, a policy in place or being given major high-level consideration.

(U) If nuclear weapons first use policy or release authority is revealed, NSC referral is also required as a waiver exception.

2. (U) Strategic Information of Continuing Critical Importance to an Ally

~~(S)~~ (b)(1); 1.4 (d)
(b)(1); 1.4 (d)

3. International Agreements Protected Past 50 Years (U)

(U) Some treaties or international agreements may, by their nature, require continued classification. Depending on the particular context, subjects may include, but are certainly not limited to, intelligence sharing, mutual defense arrangements, aid to regions still in conflict, or technical annexes with specific military base, deployment or other details that, if released, would jeopardize those agreements. See the Red Book for possible L/T referral and / or pre-release notification requirements. In addition to the treaty or agreement text that remains classified, exemption must be extended to relevant background and negotiating documents and exchanges that reveal classified information.

(U) Meanwhile, reviewers are authorized to extend the classification on any agreement that includes special classified military arrangements or contingency commitments or arrangements still in force.

(U) This authority does not extend to agreements that simply discuss compensation or funding arrangements for past military base arrangements, or outdated agreements which the governments on both sides have changed or updated, unless declassification would cause serious harm to current U.S. foreign relations or activities.

(U) If evoking Section 3.3(h) authority to extend exemption from declassification beyond 50 years for records described in this section, reviewers should exempt under both (6) and (9) as: 50X6/9 and also refer to the OSD if appropriate.

4. (U) Information That Would Cause Serious Harm to U.S. Relations with a Foreign Government

(U) Such information should be carefully evaluated. Potential serious harm must be clear and specific. While it is not possible to foresee every instance in which such protection is required, the following Section 3.3(h) exemptions are authorized. Any additional extended exemption should be specifically approved at the level of an Assistant Secretary of State.

~~(S)~~ (b)(1); 1.4 (c); 1.4 (d)
(b)(1); 1.4 (c); 1.4 (d)

~~(S)~~(b)(1); 1.4 (c)

(b)(1); 1.4 (c)

~~(S)~~ Information that reveals or suggests significant U.S. threats or “arm twisting” of a foreign government that is likely to evoke a serious negative reaction in the government or public opinion of the country concerned should be exempted beyond 50 years.

(U) Comments by or reporting on a foreign leader that makes frank, derogatory comments about another nation’s leader(s) may be exempted from automatic declassification beyond 50 years if release would cause serious harm to current U.S. foreign relations. Changes of government and leaders over 50 years will make the requirement to exempt such material beyond 50 years rare.

5. (U) Weapons of Mass Destruction

(U) Section 3.3(h) authority is limited to extending the exemption from declassification to “key design concepts of weapons of mass destruction.” Since the Atomic Energy Act supersedes the Executive Order with regard to all nuclear information, State reviewers should refer all marked RD and “possible RD” documents to the DOE regardless of the date of the document. Reviewers should refer marked FRD and “possible FRD” documents to OSD regardless of the date of the document.

(U) The Department has a direct equity in classified information relating to the past, present, or planned presence of U.S. nuclear weapon storage sites in foreign countries. In those relatively few instances where the fact of a nuclear presence is still highly sensitive and declassification could seriously harm current U.S. foreign relations and activities, reviewers should apply a 50X6 exemption whether or not the documents are marked RD, FRD, or unmarked. Unmarked documents containing such information should be referred to OSD as “possible FRD.” OSD will evaluate the FRD designation and refer to the appropriate agencies for NSI review prior to declassification. At that time, State may reconsider the 50X6 exemption.

(U) Records containing information on other weapons of mass destruction (e.g., chemical, biological) should be referred to the Army.

**C. (U) STATUTES, TREATIES, & INTERNATIONAL AGREEMENTS
50X9**

(U) For extended discussion of protection of most classified international agreements, see paragraph III.C.3 above.

(U) In some instances, such as the SCC for strategic arms control, there is a formal agreement that both sides must approve before release of the Commission's minutes and deliberations. Presumably most such material will have been released prior to 50 years, or a decision will have been made unilaterally to release.

(U) If not, approval to release unilaterally should be sought from the Assistant Secretary of State most involved with the issue, as well as L/T.

(U) NATO: NATO registry documents shall be governed by the agreements on release of such documents. Purely State Department equities concerning NATO shall only be withheld beyond 50 years if they fall under the exemptions authorized elsewhere in Part III of this Guide.