



governmentattic.org

"Rummaging in the government's attic"

Description of document: Department of Justice (DOJ) Justice Management Division (JMD) Declassification Guide, 2018

Requested date: 31-March-2020

Release date: 01-June-2021

Posted date: 14-August-2023

Source of document: FOIA Request
Justice Management Division
Department of Justice
Room 1111 RFK, 950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
Email: JMDFOIA@usdoj.gov

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.



U.S. Department of Justice
Justice Management Division
Office of General Counsel

Washington, D.C. 20530

RE: JMD FOIA # 123688

I am responding on behalf of the Justice Management Division (JMD) to your Freedom of Information Act (FOIA) request dated March 31, 2020, for a copy of the Department of Justice Declassification Guide dated 12/3/2018 and approved by ISCAP.

Enclosed is the document we believe is responsive to your request, although it is dated September 6, 2018. There are a few redactions under Exemptions 6 for certain personally identifiable information. We have determined that the privacy interests outweigh the public interest in disclosure of such information.

You may contact our FOIA Public Liaison, Karen McFadden at (202) 514-3101 or JMDFOIA@usdoj.gov for further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with JMD's determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,
MORTON
POSNER

Morton J. Posner
Deputy General Counsel

Digitally signed by MORTON
POSNER
Date: 2021.06.01 14:52:59
-04'00'



**UNITED STATES DEPARTMENT OF JUSTICE
DECLASSIFICATION GUIDE**
FOR USE IN THE REVIEW AND DECLASSIFICATION OF RECORDS UNDER
EXECUTIVE ORDER 13526, "CLASSIFIED NATIONAL SECURITY INFORMATION"

Version 2

September 6, 2018

APPROVED BY: James L. Dunlap
Department Security Officer
Justice Management Division

DATE: September 6, 2018

TABLE OF CONTENTS

(U) DOCUMENT CHANGE LOG..... 3

(U) GENERAL INFORMATION 4

 (U) PURPOSE AND SCOPE 4

 (U) AUTHORITIES..... 5

 (U) RESPONSIBILITIES FOR MAINTAINING THE GUIDE..... 5

 (U) EXEMPTION CATEGORIES 5

 (U) MANDATORY DECLASSIFICATION REVIEWS AND FREEDOM OF INFORMATION ACT REVIEWS..... 6

 (U) ATOMIC ENERGY ACT 7

 (U) FILE SERIES EXEMPTIONS 7

 (U) COMPROMISED INFORMATION..... 9

(U) PROCEDURAL REQUIREMENTS..... 10

 (U) MARKING 11

 (U) REFERRALS 11

(U) NATIONAL SECURITY DECLASSIFICATION/EXEMPTION TABLES 12

 (U) ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION 12

 (U) 25X1 - INTELLIGENCE SOURCES AND METHODS 19

 (U) 50X1-HUM 20

 (U) 25X2 – WEAPONS OF MASS DESTRUCTION 26

 (U) 50X2-WMD..... 27

 (U) 25X3 – U.S. CRYPTOLOGIC SYSTEMS OR ACTIVITIES..... 28

 (U) 25X4 – STATE OF THE ART TECHNOLOGIES IN U.S. WEAPONS SYSTEMS 28

 (U) 25X5 – U.S. MILITARY WAR PLANS..... 28

 (U) 25X6 - FOREIGN RELATIONS 29

 (U) 25X7 - PROTECTION OF THE PRESIDENT AND OTHER OFFICIALS..... 34

 (U) 25X8 – EMERGENCY PREPAREDNESS & VULNERABILITIES OF INSTALLATIONS AND INFRASTRUCTURE 35

 (U) 25X9 – STATUTES, TREATIES, OR INTERNATIONAL AGREEMENTS..... 36

 (U) FURTHER EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION AT 50 YEARS 37

(U) GENERAL INFORMATION

(U) PURPOSE AND SCOPE

(U) Executive Order (E.O.) 13526, “Classified National Security Information,” establishes a uniform system for classifying, safeguarding, and declassifying national security information. The purpose of the Department of Justice (DOJ) Declassification Guide hereafter referred to as “the Guide,” is to provide authoritative guidance for implementing DOJ declassification policy for historically valuable permanent records 25 years or older that contain classified national security information. The Guide should be used in conjunction with the DOJ’s National Security Classification Guide, and other valid DOJ classification/declassification guides that deal with specialized subjects.

(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 officially 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 Executive Order (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 receive 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 statutes or restrictions may apply before the information may be publically released.

(U) The Guide is the standard reference for declassification determinations within the DOJ for collateral classified information. The Guide does not provide classification guidance or protection for DOJ information that is SCI or SAP, this information will be referred to the appropriate other government agency with purview over that specific category of information.

(U) The Guide is approved for use by DOJ personnel specifically authorized, trained and tasked with declassifying national security information, including equity identification, on behalf of the DOJ.

(U) Nothing in this Guide prevents officials who hold original classification or declassification authority from exercising discretionary authority to declassify information over which they have purview.

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

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

(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.

(U) NOTE: Due to the uniqueness of their mission and historical precedent, the Federal Bureau of Investigation (FBI) is responsible for the operation of their automatic declassification program, including review of their classified equities. The FBI maintains their own automatic declassification guide and file series exemptions. Unless provided specific authorization and guidance, DOJ declassification reviewers are not authorized to make decisions on FBI originated information. This Guide covers and includes all DOJ components except the FBI, which has its own guide.

(U) AUTHORITIES

(U) The Guide has been prepared in accordance with the requirements and criteria set forth in E.O. 13526, 32 C.F.R. Part 2001, and the DOJ Security Program Operating Manual (SPOM).

(U) RESPONSIBILITIES FOR MAINTAINING THE GUIDE

(U) The Security and Emergency Planning Staff, Office of Information Safeguards and Security Oversight (SEPS/OISSO) is responsible for producing and maintaining the Guide. DOJ personnel with questions or comments on the Guide should contact SEPS/OISSO at [REDACTED] or [REDACTED]. SEPS is also responsible for conducting declassification reviews and providing training to declassification reviewers. With the exception of the FBI, all DOJ components are required to coordinate their declassification efforts with and through SEPS.

b(6)

(U) If information meets the criteria for continued classification and it does not appear as an exemption in the Guide, or any other relevant declassification guide-contact the SEPS/OISSO for guidance. Interagency Security Classification Appeals Panel (ISCAP) approval will be required if a new category of information is proposed for exemption from automatic declassification. The Guide will be updated as circumstances require, but at least every 5 years in coordination with the ISCAP. Proposed change requests and updates to the Guide must be coordinated through SEPS/OISSO. SEPS/OISSO will submit a letter of justification to the ISCAP amending the Guide. Pending receipt of a response from ISCAP, the documents containing the information in question will remain classified. Any information already 25 years old and not covered by this Guide will be automatically declassified.

(U) EXEMPTION CATEGORIES

(U) E.O. 13526 provides for Automatic Declassification for all classified records that are 25 years or older and have been determined to have permanent historical value under Title 44, USC, *unless* the information has been deemed exempt from automatic declassification because it falls into one of the following categories:

1. Reveal the identity of a confidential human source, or a 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 (25X1);
2. Reveal information that would assist in the development, production, or use of weapons of mass destruction (25X2);
3. Reveal information that would impair U.S. cryptologic systems or activities (25X3);

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

4. Reveal information that would impair the application of state-of-the art technology within a U.S. weapon system (25X4);
5. 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 (25X5);
6. 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 (25X6);
7. 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 the national security, are authorized (25X7);
8. Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security (25X8); or
9. Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years (25X9).

(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 a 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.

(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 year old 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).

(U) Declassification does not equate public release of information. Material that no longer merits protection under the terms of E.O. 13526 may 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 (FOIA) exemptions, the Privacy Act (PA) of 1974, and the National Security Act of 1947, as amended.”

(U) As the Attorney General is the chief law enforcement officer of the Federal Government, most prevalent among DOJ records is law enforcement information [the (b)(7)s]. Exemption 7 of the FOIA protects from disclosure “records or information compiled for law enforcement purposes,” the release of which:

- a) Could reasonably be expected to interfere with law enforcement proceedings,
- b) Would deprive a person of a right to a fair trial or an impartial adjudication,

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

- c) Could reasonably be expected to constitute an unwarranted invasion of personal privacy,
- d) Could reasonably be expected to disclose the identity of a confidential human source,
- e) Would disclose techniques, procedures, or guidelines for investigations or prosecutions, or
- f) Could reasonably be expected to endanger an individual's life or physical safety.

(U) Declassification reviewers will frequently encounter law enforcement information that may have been erroneously marked as classified national security information. For example, law enforcement or criminal confidential human sources are not classifiable unless there is also a specific national security connection to their reporting. Though a criminal confidential human source or informant identity is extremely sensitive, this information may not be classified as national security information. This information would instead be properly withheld under the FOIA (b)(7)(d) exemption.

(U) ATOMIC ENERGY ACT

(U) Documents containing or potentially containing Restricted Data (RD) or Formerly Restricted Data (FRD) are not subject to the automatic declassification provisions of E.O. 13526. Nothing in this Guide shall be construed as providing for declassification of this information. All marked RD and any unmarked information that is suspected to be RD must be referred to the Department of Energy (DOE) for declassification review. All marked FRD and any unmarked information that is suspected to be FRD must be referred to the DOE and the Department of Defense (DoD) for declassification review.

(U) Any DOJ declassification reviewer who believes they have located unclassified or classified information that properly should have been classified under the Atomic Energy Act shall refer the document to the DOE.

(U) ALL DOJ declassification reviewers are required to have both a "Q" clearance and have attended and passed the DOE Historical Records Restricted Data Reviewers (HRRDR) 4-day course.

(U) FILE SERIES EXEMPTIONS

(U) With the exception of the FBI, the National Security Division (NSD) is the only DOJ component with ISCAP approved file series exemptions. Specific NSD (formerly the Office of Intelligence Policy and Review) operational file series have been determined to almost invariably contain information that falls within one or more of the exemption categories under section 3.3(b) of E.O. 13526. These records remain exempt 50 years from the date of origin and will undergo systematic declassification review in the year the oldest records become 45 years old (2024). Records exempted from automatic declassification under a file series exemption remain subject to mandatory declassification review under section 3.5 of E.O. 13526.

(U) ISCAP has approved the following NSD operational file series exemptions related to foreign intelligence, counterintelligence, and international terrorism investigations:

1. Foreign Intelligence Surveillance Act of 1978 (FISA) Files

The FISA, as amended, prescribes procedures for the physical and electronic surveillance and collection of foreign intelligence information regarding persons or entities suspected of being foreign powers or agents of foreign powers. Foreign powers and agents of a foreign power are defined in FISA to include international terrorist organization and their members and supporters, as well as foreign governments and their officers and employers.

All applications for FISA authority presented to the Foreign Intelligence Surveillance Court (FISC) must be approved by the AG. The FISC may authorize electronic surveillance, issue physical search warrants, pen registers and trap and trace orders, and orders to obtain tangible items including business records, tax returns, education and medical records (commonly called business record orders). FISA also imposes narrow restrictions on a court's authority to order disclosure of FISA applications, orders, and related material. This is necessary because FISA materials contain highly-classified information the disclosure of which could seriously harm national security.

These "FISA Files" include incoming requests to initiate collection activity; AG certifications authorizing electronic surveillance; applications to the FISC for electronic surveillance and court orders authorizing surveillance; letters of approval from the Director of Central Intelligence and National Security Advisor; draft documents, related memoranda, motions, affidavits, filings, correspondence, and electronic communications; and other related documents or records. All of the material within these files relates directly to intelligence activities, sources, and methods, and much of the material consists of Sensitive Compartmented Information (SCI) received from other agencies within the Intelligence Community (IC).

2. *Intelligence Community Operations Files*

This file series includes records created in the course of OIPR (NSD's predecessor) fulfilling DOJ's responsibilities under P.L. 102-140, E.O.s 12333 and 12356, and internal AG guidelines. These include proposals from intelligence community agencies seeking AG authorization, approval or concurrence on a variety of operational matters, including covert actions, electronic surveillance and physical search abroad, testing of equipment in the United States and use of new technologies. These operations files may include an incoming request to initiate certain intelligence activity, decision memorandums, and the AG's (or designee) approval. All of the material within these files relates directly to intelligence activities, sources, and methods, and much of the material consists of SCI received from other agencies within the IC.

3. *E.O. 12333 2.3 and 2.5 Files*

Sections 2.3 and 2.5 of E.O. 12333, "United States Intelligence Activities," authorize the application of certain foreign intelligence and counterintelligence collection methods to United States persons, and foreign powers and their agents under certain circumstances. Pursuant to sections 2.3 and 2.5, the President has delegated to the AG the authority to approve requests for the application of these methods. These "2.3 and 2.5 Files" may include an incoming request to initiate collection activity, request memorandum to the AG, and the AG's letter of approval, and all related memoranda, motions, affidavits, filings, correspondence, and electronic communications. All of the material within these files relates directly to intelligence activities, sources, and methods, and much of the material consists of SCI received from other agencies within the IC.

4. *Mail Cover and Undercover Files*

The Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1993, Public Law 102-395, as extended by Public Law 104-132, Section 815(d) (April 24, 1996), and the various sets of AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection authorize and regulate certain national security and intelligence activities by the FBI. The "Mail Cover and Undercover Files" may include an

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

incoming request and approval memorandum for mail covers, undercover leases and purchases of property, certain travel and physical searches. All of the material within these files relates directly to intelligence activities, sources, and methods, and much of the material consists of SCI received from other agencies within the IC.

(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 Executive Order (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 before the Congress by U.S. Government officials;
- 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) alerting 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

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

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.").

(U) PROCEDURAL REQUIREMENTS

(U) The main objective of document review is to declassify as much information as possible without compromising national security. Personnel assigned the responsibility to conduct a declassification review will examine each document, page-by-page and line-by-line. When classified information is

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

reviewed it may be declassified in full, remain classified in full under appropriate ISCAP approved exemption category, declassified as redacted (segregated), excluded (RD/FRD), and/or referred to another government agency for further review or disposition. For records in DOJ custody, final approval for release in any form, however, always rests with a U.S. Government releasing authority. Declassified material may not be released to the public until it is reviewed under the provisions of the FOIA, PA, and other relevant statutes, to ensure that no legally protected, privileged or personal material is released.

(U) MARKING

(U) If 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), as specified by the Information Security Oversight Office (ISOO). **NO MARKINGS SHALL BE MADE ON THE DOCUMENT.** The SF-715 shall be marked with all appropriate information, including referral to other agencies and change in classification, if required.

(U) All relevant categories (1) through (9) of section 3.3(b) of E.O. 13526 shall be indicated on the SF-715 as “25X1”, “25X6”, etc. to certify withholding beyond 25 years from the date of the document. For those rare instances in which a document is to be classified beyond 50 years due to the identity of a human intelligence source, the designation would be 50X1-HUM. Documents being reviewed in electronic format will have the same information as specified on the SF-715, entered as provided in the computer program.

(U) Only 25X exemptions may be applied to records reviewed in anticipation of automatic declassification at 25 years. Other than the 50X1-HUM and 50X2-WMD exemptions, 50X exemption may only be applied to records approaching automatic declassification at 50 years. 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 a 50X exemption is later applied 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.

(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 an ISOO Notice, available on www.archives.gov/isoo/notices.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

(U) NATIONAL SECURITY DECLASSIFICATION/EXEMPTION TABLES

(U) ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION

(U) The following items of information are automatically declassified 25 years after their original classification date. Information in the legal custody of DOJ declassified pursuant to this Guide may be withheld from public disclosure pursuant to appropriate FOIA and Privacy Act exemptions.

TABLE 1.1 ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
ITEM #	DESCRIPTION	COMMENTS
1	(U) Information NOT considered national security in nature.	(U) Declassification reviewers will frequently encounter law enforcement information that may have been erroneously marked as classified national security information. For example, law enforcement or criminal confidential human sources are not classifiable unless there is also a specific national security connection to their reporting. Though a criminal confidential human source or informant identity is extremely sensitive, this information may not be classified as national security information. This information would instead be properly withheld under the FOIA (b)(7)(d) exemption.
2	(U) Information the content or context of which is NOT source revealing.	
3	(U) Source reporting on Criminal and Law Enforcement matters ONLY.	(U) Unless there is an identifiable national security nexus to the source reporting, Criminal and Law Enforcement sources are unclassified. This information should not have been classified in the first place, and when found, should be declassified immediately. Criminal and Law Enforcement source information can be withheld and protected under the appropriate FOIA (b)(7) exemptions.
4	(U) Information made public as part of a trial.	(U) While some case information regarding civil litigation or criminal prosecution may require continued classification, information that has been publicly revealed in court documents should be declassified.
5	(U) National Security aspects of the overall DOJ mission.	
6	(U) The legal basis for DOJ national security activities.	(U) This includes the limitations created by the Constitution, statutes, case law, and Government directives (such as Executive Orders) that are themselves unclassified.
7	(U) General discussions of the categories of national security intelligence.	(U) For example, counterterrorism, counterintelligence, other varieties of foreign intelligence and their distinctions from criminal intelligence.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1 ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
8	(U) DOJ priorities within national security missions and objectives, including both operations and intelligence.	(U) At a level of generality that does not identify particular persons, organizations or foreign countries as subjects of DOJ investigations.
9	(U) General discussions of the role that counterterrorism intelligence plays in the overall counterterrorism mission.	
10	(U) Identification of the <u>general</u> subject matter of a counterterrorism threat assessment.	
11	(U) The criteria for opening, continuing, or closing a national security investigation.	(U) Includes the distinctions among threat assessments, preliminary investigations, and full investigations.
12	(U) Identification of categories of information that shall be shared, may be shared, or have been shared with state, tribal and local law enforcement authorities and personnel.	(U) DOJ originated information may carry the caveat “For Official Use Only” FOUO if recipient law enforcement personnel are authorized to share it with other state and local officials, or “Law Enforcement Sensitive” (LES) if it is not to be shared outside of the law enforcement and public safety communities.
13	(U) Identification of categories of information that may not be shared with particular categories of people or organizations.	
14	(U) Domestic distribution lists for intelligence products, identifying offices but not names of persons.	
15	(U) List of names of DOJ employees identifying them as DOJ employees.	
16	(U) Definition of a “threat country” and the fact that a list of these countries is maintained.	
17	(U) Discussions of the differences among a threat assessment, a preliminary investigation, and a full investigation in terms of the available investigative techniques-where such declassification will not disclose intelligence targets, techniques, sources or methods that are classified for other reasons.	(U) This applies only when NOT linked to a specific case and to general discussion level of information found in unclassified guides such as the “FBI Domestic Investigation and Operations Guide” or other Attorney General Guidelines.
18	(U) Identification of the general subject matter of a threat assessment dealing with a national security threat other than international terrorism.	
19	(U) Positive results or findings of a threat assessment, preliminary investigation, or full investigation dealing with international terrorism.	(U) Refers to identification of a person or group as terrorist or supportive of terrorism when isolated from the reason why. Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
20	(U) Negative findings of a threat assessment, preliminary investigation or a full investigation.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1		
ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
21	(U) Discussions of the criteria and approval process for opening or closing a threat assessment, a preliminary investigation or a full investigation, where declassification will NOT disclose intelligence targets, techniques, sources, or methods classified for other reasons.	(U) This applies only when NOT linked to a specific case.
22	(U) Information regarding the incentives that were or may have been offered to a confidential human source reporting on national security matters.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
23	(U) Any indication that the DOJ has a source reporting on an identified individual or group, if this report is part of a national security investigation related to proliferation, infrastructure protection, narcotics, or other foreign intelligence or foreign counterintelligence matters other than terrorism or espionage.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
24	(U) Information pertaining to an <i>officially acknowledged</i> source.	
25	(U) General Discussions, not related to a specific case, of investigative techniques that may be available to the DOJ.	(U) This includes discussions of their advantages and disadvantages. HOWEVER, identification of any techniques or methods that would enable subjects of investigation to evade or degrade all available investigative techniques is exempt from declassification if such techniques or methods would be effective under current conditions. Also includes lessons drawn from past experience when not linked to specific past cases. This does not apply to investigative techniques that are themselves classified.
26	(U) Identification of an investigative technique that has been used in a specific case.	(U) This does not apply if: - The technique is in current use and is currently classified; or - There is another reason for classifying this information.
27	(U) Identification of investigative techniques that have not been used, or are not intended to be used, in a specific national security cases or a defined category of national security cases.	(U) This does not apply if: - The technique is in current use and is currently classified; or - There is another reason for classifying this information.
28	(U) Discussions of the advantages and disadvantages of using specific investigative techniques in a specific national security case.	(U) This applies whether the decision to use a specific technique is affirmative or negative. (U) This does not apply if: - The technique is in current use and is currently classified; or - There is another reason for classifying this information.
29	(U) Techniques officially acknowledged.	

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1		
ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
30	(U) <u>Generic</u> discussions of investigative techniques (not linked to a particular investigation or group of investigations) that require a FISA warrant. Such discussions may go to the level of detail used by the DOJ in published documents, public legal proceedings, and unclassified testimony to Congress.	(U) HOWEVER, identification of any techniques or methods that would enable subjects of investigation to evade or degrade all available investigative techniques is exempt from declassification if such techniques or methods would be effective under current conditions. Moreover, exemption from declassification is appropriate if: - The investigative technique is in current use and is currently classified; or - There is another reason for classifying this information.
31	(U) With NO additional or specific details, the number of applications for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes made to the Foreign Intelligence Surveillance Court (FISC) during a calendar year.	(U) This information is published in DOJ's UNCLASSIFIED reports to Congress pursuant to sections 107 and 502 of the FISA, 50 USC § 1801 <i>et seq.</i> , and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005. See section 107 of the Act, 50 U.S.C. § 1807.
32	(U) With NO additional or specific details, the number of applications for access to certain business records (including the production of tangible things) made to the FISC during a calendar year.	(U) This information is published in DOJ's UNCLASSIFIED reports to Congress pursuant to sections 107 and 502 of the FISA, 50 USC § 1801 <i>et seq.</i> , and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005. See section 502 of the Act, 50 U.S.C. § 1862(c)(1).
33	(U) With NO additional or specific details, the number of requests made for certain information concerning different United States persons pursuant to National Security Letter Authorities during a calendar year.	(U) This information is published in DOJ's UNCLASSIFIED reports to Congress pursuant to sections 107 and 502 of the FISA, 50 USC § 1801 <i>et seq.</i> , and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005. See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (2006).
34	(U) With NO additional information or specific details, the numbers of pen registers and trap and trace devices used by the law enforcements agencies of the DOJ during a calendar year.	(U) This includes the number of original orders, extensions, number of investigations, number of persons whose telephone facilities were affected, and number authorized for email/networks.
35	(U) General discussions of the benefits and risks of international cooperation.	(U) Includes generic discussion of sharing intelligence.
36	(U) Any indication that the DOJ has a source reporting on an identified individual or group, if the report is part of an <u>economic</u> counterintelligence or <u>economic</u> espionage investigation.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
37	(U) Identification of a specific individual or organization other than a threat country or an individual or group operating under the direction of a threat country as the subject of an <u>economic</u> counterintelligence or <u>economic</u> espionage investigation-whether it is a threat assessment, a preliminary investigation, or a full investigation.	

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1 ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
38	(U) Information which would enable an inference identifying a specific individual or organization other than a threat country or an individual or group operating under the direction of a threat country as the subject of an <i>economic</i> counterintelligence or <i>economic</i> espionage investigation-whether it is a threat assessment, a preliminary investigation, or a full investigation.	
39	(U) Internal DOJ discussion about whether to open or close a particular <i>economic</i> counterintelligence or <i>economic</i> espionage case in which a threat country is not a major focus.	
40	(U) Identification of the person or organization referred to by a code word in the context of an <i>economic</i> counterintelligence or <i>economic</i> espionage case in which a threat country is not a major focus.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
41	(U) The identification of the subject of an <i>economic</i> counterintelligence or <i>economic</i> espionage investigation in which a threat country is not a major focus, when that investigation is being carried out in cooperation with one or more foreign governments.	(U) Where such declassification will not disclose intelligence targets, techniques, sources, or methods that are classified for other reasons.
42	(U) Information that at the time of its creation would have allowed an adversary of the U.S. to neutralize, access or destroy systems or capabilities, but which because of the passage of time would no longer do so.	(U) When reviewing this category of information, declassification reviewers must consider whether the passage of time has rendered any possible risk obsolete prior to making the decision to declassify or exempt.
43	(U) Information regarding any form of covert communications used by international terrorists or those suspected of being international terrorists.	(U) This includes the fact that a covert communication was used, or might be used, in a specific circumstance. This includes the technology, techniques, or equipment used for such communications. (U) Where declassification will not disclose intelligence targets techniques, sources, or methods that are classified for other reasons.
44	(U) Identification of <u>generic</u> terrorist threats that the DOJ has technical capabilities to counter, where such declassification will not provide information about threats that the DOJ may not be able to counter.	(U) Where declassification will not disclose intelligence targets techniques, sources, or methods that are classified for other reasons.
45	(U) Detailed itinerary of AG or other senior DOJ official's travel plans.	

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1		
ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
46	<p>(U) The following information on an individual included (or to be included) in a terrorist watch list:</p> <ul style="list-style-type: none"> - Name and aliases - Date of birth - Place of birth - Alien registration number, visa number(s), social security account number, or other unique identifying number(s) - Passport information - Country of origin and nationality or nationalities - Physical identifiers, such as sex, race, height, weight, eye color, hair color, scars, marks or tattoos - Known locations, such as addresses or points of travel, including prior admissions to the United States - Photographs or renderings - Fingerprints or other biometric data - Employment data - Phone number(s) and license plate numbers 	
47	(U) National security investigation case numbers.	(U) All material associated with a particular national security case number must be carefully reviewed to ensure that declassification of the case number will not facilitate identification of the specific threat country, and or organization to which the case number refers, if the specific case number remains in use.
48	(U) Code words created to conceal the identity of the subject of a national security investigation when not linked to the actual identity.	(U) All material associated with a particular code word must be carefully reviewed to ensure that declassification of that code word will not facilitate identification of a source or technique.
49	(U) Identification of a specific individual or organization as the subject of a national security investigation when this identification has been made public under proper authority.	(U) Examples include public statements by senior officials or an arraignment at which the individual is charged with espionage. Such identifying information would still be classified if it reveals an additional subject identity that is not public or if classified for other reasons.
50	(U) Identification of a specific individual or organization as the subject of an international terrorism matter, whether it is a threat assessment, a preliminary investigation, or a full investigation.	(U) Where such declassification will not disclose intelligence targets, techniques, sources or methods that are classified for other reasons.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.1 ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
51	(U) The reasons for opening an international terrorism investigation of an identified person or group.	(U) Where such declassification will not disclose intelligence targets, techniques, sources or methods that are classified for other reasons. This applies to cases that have been closed as well as to open cases.
52	(U) Information that would enable an inference identifying a specific individual or organization as the subject of an international terrorism matter, whether it is a threat assessment, a preliminary investigation, or a full investigation.	(U) This applies to cases that have been closed as well as to open cases. Where such declassification will not disclose intelligence targets, techniques, sources or methods that are classified for other reasons.
53	(U) Internal DOJ discussion about whether to open or close a particular international terrorism case.	
54	(U) DEA sourced information on narcotics production and demand; trafficking developments; crop estimates; incentives behind narcotics production; transnational drug sources; interdiction; drug safe havens; trafficking routes (air, maritime, overland); and trafficking trends.	(U) The passage of time negates the continued sensitivity of this information.
55	(U) Information on narcotics arrests and/or convictions.	
56	(U) General information on narcotics initiatives with foreign governments.	(U) Cooperation with foreign governments on narcotics issues is normally widely publicized. However, specific details beyond general information should be examined in accordance with "Table 1.3 – 25X6 Foreign Relations" for possible exemption.
57	(U) General statements on narcotics related foreign government corruption.	(U) This would include statements that governments are reforming their police forces to reduce corruption, that corruption exists within a particular foreign government, or allegations of corruption with no specific identification of those suspected. However, specific details beyond general information should be examined in accordance with "Table 1.3 – 25X6 Foreign Relations" for possible exemption.
58	(U) General information on coordinated aid programs and narcotics training provided to foreign governments.	(U) The fact that the DEA conducts international counter-narcotics training is not classified. The DEA provides assistance to foreign governments seeking to develop narcotics law enforcement programs, organizational infrastructures, and judicial reforms.

U.S. Department of Justice
 Justice Management Division
 Security and Emergency Planning Staff

TABLE 1.1 ITEMS AUTOMATICALLY DECLASSIFIED 25 YEARS AFTER ORIGINAL CLASSIFICATION		
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 DECL-item #		
59	(U) General information on narcotics challenges faced in a specific geographic location or area.	(U) For example, the fact that the cultivation, production, trafficking, and consumption of illicit drugs flourish in Afghanistan or that traffickers provide weapons, funding, and other material support to the insurgency in exchange for the protection of drug trade routes, cultivation fields, laboratories, and trafficking organizations is not classified. Information of this nature is widely published in various unclassified U.S. Government Narcotics Reports. However, specific details beyond general information should be examined in accordance with “Table 1.3 – 25X6 Foreign Relations” for possible exemption.

(U) 25X1 - INTELLIGENCE SOURCES AND METHODS

E.O. 13526, Section 3.3(b)(1): “Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.”

(U) Information concerning intelligence sources and methods is commonly located in DOJ records. As the chief law enforcement officer of the Federal Government, the Attorney General represents the United States in legal matters generally, gives advice and opinions to the President and to the heads of executive departments of the Government concerning the legality of intelligence related activities, and interprets relevant intelligence statutes, executive orders, and presidential directives. However, with the exception of those DOJ components who are members of the Intelligence Community (the FBI Intelligence Branch and the DEA Office of National Security Intelligence), DOJ is largely a consumer vice originator of classified information regarding intelligence sources and methods. As consumers of intelligence information, most DOJ records containing intelligence information are derivatively classified and must be referred to the appropriate equity agency(ies) in accordance with section 3.3(d)(3) of E.O. 13526.

(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 relationship, or both, are to be held in confidence. The understanding that there is to be confidentiality need not be explicit. If there is a determination that information was passed in the expectation of confidentiality, the decision to exempt from declassification need not focus on the specific individual or the sensitivity of the information passed if just divulging the source would be likely to damage confidence in the willingness of the U.S. to protect sources of information. Conversely, there is no need to protect information provided by a confidential source if the information itself does not reveal the source’s identity, or reveal information about the application of an intelligence source or method.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

(U) It is not necessary that a confidential human source be named if the description would allow reasonable identification of the individual from the title or information provided. Often the sensitivity of protecting a source ends with the source's death, but this is not always the case. There may be circumstances where revealing information can lead to retribution to the source's group or family, or seriously compromise the willingness of current officials or individuals to share information in confidence with the U.S. However, even when a document says "protect source," this is not an automatic exemption and it may indicate that protection was only needed for a limited duration.

(U) Excluding the FBI, all DOJ classified information in records from 45 years or older that does not reveal the identity of a confidential human source or human intelligence source and fall under the 50X1-HUM exemption will be automatically declassified. All other intelligence sources and methods information will be referred to the appropriate equity agency(ies) or declassified/exempted (25X1) in accordance with the instructions contained in this Guide. 50X1-HUM exemptions automatically expire when the information becomes 75 years of age in accordance with section 3.3(h) of E.O. 13526.

(U) 50X1-HUM

Executive Order 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 could 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."**

(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. This authority should be used sparingly by DOJ reviewers, since in most cases 50 years will have been sufficient to protect most of our sources. However, in cases where the individual in question was sufficiently young at the time of the incident requiring protection and may still be professionally active, or in cases in which the nature of the authoritarian regime is such as to bring possible repercussions upon an individual, family, or organization, protection beyond 50 years should be considered. Reviewers should then pick a date for declassification that is 75 years from the document date and record the exemption as 50X1-HUM. Information that reveals human intelligence sources should be referred to the intelligence community element concerned for protection.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2 25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
1	(U) The name of an individual (identity) who has provided or may reasonably be expected to provide, information to the DOJ on matters pertaining to national security with the expectation that the information or the relationship, or both, are to be held in confidence.	50X1-HUM	(U) The identity of a human source could be revealed by name, title of position, description of activity, placement at a certain location at a certain time, isolation in a small group of individuals with unique knowledge of the information, or similar information that would logically permit the identification of the source.
2	(U) The name of an organization <i>may be exempted if, and only if</i> , the identity of the organization could reasonably be expected to lead to the identity of a current confidential human source or a current human intelligence source. This could, in some instances, include information that would allow the name of an organization to be inferred.	50X1-HUM	(U) Organization often refers to a company or an identifiable subdivision of a large company. This also applies to characteristics or other data that could reasonably be expected to identify the organization. (U) Reviewers must be able to identify at least one scenario or circumstance in which knowledge of the name of the organization in question would lead to the identity of a current human intelligence source.
3	(U) The name of an organization (or information that would allow the name to be inferred) that is cooperating with the DOJ with an expectation of confidentiality if the identity of the organization could NOT reasonably be expected to lead to the identity of a confidential human source.	25X1	(U) Organization often refers to a company or an identifiable subdivision of a large company. This also applies to characteristics or other data that could reasonably be expected to identify the organization.
4	(U) Relationships and operational support contracts with persons, or such relationships and support contracts with companies, corporations, or universities as allow the inference of the identities of cooperating persons, in connection with national security investigations.	25X1	
5	(U) Information regarding non-human intelligence sources and methods when the particular circumstances mean that this information could reasonably be expected to lead to the identification of a confidential human source.	25X1	
6	(U) Discussions of the advantages/disadvantages of attempting to recruit a specific individual or organization as a source on a national security matter.	25X1	

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2 25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
7	(U) Any indication that the DOJ has a source reporting on an identified individual, if this report is part of an unacknowledged international terrorism investigation.	25X1	
8	(U) Any indication that the DOJ has a source reporting on an identified individual or group, if this report is part of an unacknowledged espionage investigation.	25X1	
9	(U) Information on techniques used in spotting, recruitment, vetting, security, handling, communications and termination of confidential human intelligence sources used in connection with national security investigations.	25X1	
10	(U) Identification of the person or organization referred to by a code word used in connection with national security investigations unless otherwise released or deceased.	25X1	
11	(U) Contractual information that reasonably could be expected to reveal confidential relationships in connection with ongoing national security investigations.	25X1	(U) This applies to contractual information regarding a relationship between the DOJ and an entity (e.g., a business) that, although not a “confidential human source,” might well suffer serious harm if the fact or nature of its support to the DOJ became known, and which therefore relies upon the DOJ to keep this relationship confidential.
12	(U) Information regarding human sources necessary to integrate collection activities of the U.S. and its allies.	25X1	(U) This does not include the names of individuals who are already confidential sources, or information that could reasonably be expected to identify such individuals.
13	(U) <i>Specific</i> details of classified relationships between the DOJ and members of the Intelligence Community.	25X1	(U) The fact that the DOJ supports the Intelligence Community is unclassified. Identification of specific DOJ actions taken to support the Intelligence Community may be exempt. Identification of DOJ investigations for which such support was provided may be exempt unless the investigation has directly led to a criminal prosecution.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2			
25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
14	(U) Description of guidelines, policies, or DOJ processes that treat investigation of, or information about, U.S. persons differently from investigation of, or information about, non-U.S. persons.	25X1	(U) This applies to any information that could reasonably be expected to enable a foreign adversary to benefit from the protections provided by law or policy to U.S. persons, by causing the DOJ to extend to their activities the presumption of U.S. person status. A policy element no longer in force is not exempt from automatic declassification.
15	(U) Information that could reasonably be expected to identify DOJ employees operating under cover in a national security investigation.	25X1	(U) Information that identifies a retired or deceased DOJ employee who previously operated under cover is NOT exempt from automatic declassification.
16	(U) Identification or description of an investigative technique used in foreign territory, other than liaison with the government having jurisdiction.	25X1	(U) This includes information obtained through such a technique that the nature of the information allows an inference regarding the technique used to obtain it.
17	(U) Unless acknowledged, the approval process, criteria, and basis for any particular decision regarding a DOJ investigation in a foreign territory, other than by liaison with the government having jurisdiction.	25X1	(U) This might also be 25X6.
18	(U) The nature of unacknowledged DOJ action taken at the request of a member of the Intelligence Community (IC).	25X1	(U) This includes the criteria and approval process, as well as the reasons for approving a particular action. Identification of DOJ investigations for which support was provided is exempt unless the investigation directly led to a criminal prosecution.
19	(U) Information about an investigative technique that is currently in use in national security investigations that would, if made public, reduce the effectiveness of the technique.	25X1	(U) This applies to details of a technique that have not been made public even when use of the technique in general has been officially acknowledged.
20	(U) Identification of particular technical capabilities used to counter generic terrorist threats provided they are still in use.	25X1	
21	(U) Association of particular capabilities with particular terrorist threats that they may be able to counter provided it is still in use.	25X1	

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2			
25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
22	(U) Information that describes or reveals the targets, tasking's, results, configurations, dates, means of disguising or hiding, capabilities, successes, weaknesses, vulnerabilities or failure of covert collection systems, methods or equipment used in connection with national security investigations or in support of other agencies in the IC.	25X1	(U) Includes information concerning specific uses of: - Extraordinary techniques (i.e., electronic surveillances, pen registers, trap and trace devices, mail openings, and physical searches) - Clandestine fixed observation sites, listening sites, technical sites, switching points and buffer zones. - Clandestine physical and photographic surveillance. - Mail and Trash covers. - Consensual monitoring - National security letters to obtain consumer information, subscriber information, toll billing records and electronic communication transactional records, financial records, and financial, consumer and travel records of certain executive branch employees. - False documentation to conceal identities. - Code words when linked to actual identities of active operations. - Accessing education records. - Accessing business records, books, papers, documents and other items. - Searches by or in conjunction with the U.S. Customs Service.
23	(U) Specific use of tracking devices, safe houses (including locations and methods used to acquire, maintain and dispose of them), cover communications methods, clandestine meeting techniques, undercover activities, and undisclosed participation, and forensic examinations within the confines of national security investigations pursuant to guidelines established by the Attorney General. ¹	25X1	(U) Exempt only when such methods, techniques, locations or devices are currently in use.

¹ (U//~~FOUO~~) In national security investigations (1) altered and obliterated writing; (2) biological tissues and fluids; (3) bombings, arsons, and other crime scenes; (4) clandestine communications and records; (5) computer intrusions; (6) DNA; (7) firearms and tool marks; (8) forged and counterfeit documents; (9) hairs, fibers, cordage, soil, glass, building materials, feathers and wood; (10) handwriting and printing; (11) hazardous chemical, biological, and nuclear materials; (12) latent fingerprints; (13) paper and ink; (14) photocopier print; (15) physical anthropology; (16) shoe, tire, and mechanical impressions; (17) typewriting; and (18) the successful circumvention of countermeasures and security techniques.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2 25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
24	(U) Devices and methods used to detect and defeat national security technical surveillance activities while these methods are still in use.	25X1	
25	(U) Information that reveals current training materials regarding national security operations or analysis; or information that reveals past methods that might compromise current training techniques, compromise sensitive collection systems or reveal relationships with specific liaison services.	25X1	
26	(U) Unless acknowledged, the identification of an investigative technique that has been used in a specific case.	25X1	
27	(U) Information regarding the use by the DOJ of covert communications techniques that are currently in use.	25X1	(U) This includes the fact that a covert communication was used, or might be used, in a specific circumstance. This also includes the technology, techniques, or equipment used for such communication.
28	(U) Identification of any techniques or methods that would enable subjects of investigation to evade or degrade available investigative techniques, when these technique or methods would still be effective under current conditions.	25X1	
29	(U) Information regarding any form of covert communications used by the subject(s) of a national security investigation not related to counterterrorism.	25X1	
30	(U) Discussions of the application of investigative techniques requiring a FISA court order or search warrant.	25X1	(U) This includes: - Descriptions of such techniques more detailed than those found in public documents or testimony; - Statistics on the frequency of use of particular techniques; - Identification of the use or non-use of specific techniques in specific cases or categories of cases; - Discussions of the advantages or disadvantages of specific techniques.
31	(U) The fact that an unacknowledged FISA warrant was applied for, or obtained in a specific case.	25X1	
32	(U) Identification of a specific individual or organization as the subject of a national security investigation making use of an acknowledged FISA warrant.	25X1	(U) This applies to individuals who may or may not be the subject of the original FISA warrant.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.2 25X1- INTELLIGENCE SOURCES AND METHODS (INT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 INT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
33	(U) Information in a national security case not related to counterterrorism that was obtained using authorities granted by a FISA warrant that would harm current operations.	25X1	(U) This refers both to information from which the additional capabilities authorized by the FISA warrant in this particular case could be inferred, and to information regarding U.S. persons that the DOJ could not lawfully have obtained without the use of FISA authorities.

(U) 25X2 – WEAPONS OF MASS DESTRUCTION

E.O. 13526, Section 3.3(b)(2): “Reveal information that would assist in the development, production, or use of weapons of mass destruction.”

(U) The DOJ does not have the authority to exempt information that would assist in the development, production, or use of weapons of mass destruction. This information originates in external agencies, particularly the Department of Energy (DOE) and the Department of Defense (DoD). However, because information in this category may appear in DOJ records, this exemption is discussed in some detail as an aid to equity recognition. Weapons of mass destruction include chemical, biological, radiological, and nuclear weapons. Information is 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 them. Refer this information for declassification review to the originating agency and/or agencies with primary interest and equity in accordance with section 3.3(d)(3) of E.O. 13526.

(U) Chemical and Biological Weapons (CBW). Any information that would assist in the acquisition, development, design, and manufacture of CBW systems and delivery systems or the development of homemade CBW systems that could be used by terrorists may be encountered in DOJ records. Documents containing such information should be referred to the originating agency, typically the appropriate component of the DoD (usually Army) in accordance with section 3.3(d)(3) of E.O. 13526. NOTE: Reporting on the activities of groups believed to be engaged in the acquisition, development, design, and manufacture of CBW systems and delivery systems would not be exempted under this category unless it included technical details of design, manufacture, etc.

(U) Radiological weapons. Classified information that would assist in the acquisition, development, design, or manufacture of a radiological weapons or its delivery systems or the development of homemade radiological weapons that could be used by terrorists may be encountered in DOJ records. Documents containing such information should be referred to the appropriate originating agency, typically DOE in accordance with section 3.3(d)(3) of E.O. 13526.

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

(U) **Nuclear Weapons.** U.S. nuclear weapons information falls under the authority of the DOE according to the terms of the Atomic Energy Act of 1954. DOE classified information falls into 3 categories: a) Restricted Data (RD); b) Formerly Restricted Data (FRD); and c) National Security Information (NSI), which is classified under the authority of the present and previous executive orders, such as E.O. 13526.

- a) (U) *Restricted Data (RD)*. RD concerns the design, manufacture, or utilization of atomic weapons, the production of special nuclear material, such as plutonium, deuterium, and uranium 235, and the use of special nuclear material in the production of energy. RD is controlled by DOE alone. A document, or information in a document, that is marked as RD is excluded from the automatic declassification provisions of E.O. 13526. Nothing in E.O. 13526 supersedes any requirement of the Atomic Energy Act.
- b) (U) *Formerly Restricted Data (FRD)*. 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. Examples of FRD include information about nuclear weapons stockpile quantities, safety, storage, and deployment. DOE shares control of FRD with DoD. A document, or information in a document, that is marked as FRD is also excluded from the automatic declassification provisions of E.O. 13526. Nothing in E.O. 13526 supersedes any requirement of the Atomic Energy Act.

(U) **ALL** DOJ declassification reviewers are required to have both a “Q” clearance and have attended and passed the DOE historical records RD reviewer 4-day course.

- c) (U) *National Security Information (NSI)*. NSI on these subjects should be referred to DOE and/or other agency(ies) with equity interest as required in accordance with Section 3.3(d)(3) of E.O. 13526. NSI in this category may include information that could reasonably be expected to assist other nations or terrorists in acquiring, designing, building, testing, or deploying nuclear weapons, including component parts or nuclear material; is identifiably intelligence on foreign nuclear weapons; or 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) Unmarked documents which a reviewer determines probably contain RD or FRD information should be so identified and referred to DOE as “probable RD” or “probable FRD,” but they may also be exempted and/or referred to other agencies as well as to DOE on the basis of NSI information in the documents. Originating historical offices frequently failed to mark RD and FRD information properly and used only NSI classifications to protect the information.

(U) 50X2-WMD

Executive Order 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 could 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*

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

b. Key design concepts of weapons of mass destruction.

(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 key design concepts of weapons of mass destruction. DOJ reviewers do not have the expertise to identify “key design concepts of weapons of mass destruction” and all information concerning weapons of mass destruction will continue to be referred to the appropriate equity agency (DOE and/or DoD) for their action.

(U) 25X3 – U.S. CRYPTOLOGIC SYSTEMS OR ACTIVITIES

E.O. 13526, Section 3.3(b)(3): “Reveal information that would impair U.S. cryptologic systems or activities.”

(U) The DOJ does not have the authority to exempt information that would impair U.S. cryptologic systems or activities. Cryptologic materials come under the control of the National Security Agency (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; cryptoperiod dates; and inventory reports of COMSEC material. Cryptographic information is commonly found in certain DOJ component records and will usually be found in Sensitive Compartmented Information (SCI) files. Refer this information for declassification review to the NSA and other agencies with primary interest and equity in accordance with section 3.3(d)(3) of E.O. 13526.

(U) 25X4 – STATE OF THE ART TECHNOLOGIES IN U.S. WEAPONS SYSTEMS

E.O. 13526, Section 3.3(b)(4): “Reveal information that would impair the application of state of the art technology within a U.S. weapons system.”

(U) The DOJ does not have the authority to exempt information that would impair the application of state-of-the-art technology within a U.S. weapons system. 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 U.S. weapons systems. This information originates in external agencies, particularly the DoD. Information in this category is not commonly found in DOJ files. Refer this information for declassification review to the appropriate DoD entity (usually Army, Navy, or Air Force), or if no specific entity can be identified, to OSD in accordance with section 3.3(d)(3) of E.O. 13526.

(U) 25X5 – U.S. MILITARY WAR PLANS

E.O. 13526, Section 3.3(b)(5): “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) The DOJ does not have the authority to exempt information that would 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. 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. Information in this category is not commonly found in DOJ files. This information originates in external agencies, particularly the Department of Defense. Refer this information for declassification review

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

to the Joint Chiefs of Staff and other agencies with primary interest and equity in accordance with Section 3.3(d)(3) of E.O. 13526. The National Security Council (NSC) declassification waiver also requires referral to the NSC of any records concerning the “authorization to use weapons of mass destruction” or U.S. policy on “first use of nuclear weapons.” Documents that discuss basic national security policy contingencies, as opposed to specific military war plans, should be evaluated and referred to NSC and OSD if appropriate in accordance with Section 3.3(d)(3) of E.O. 13526.

(U) 25X6 - FOREIGN RELATIONS

E.O. 13526, Section 3.3(b)(6): “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) E.O. 13526, Section 6.1(s) defines Foreign Government Information (FGI) as:

1. Information provided to the United States Government by a foreign government or governments, in 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) Although the DOJ plays a limited role in the conduct of foreign affairs and foreign diplomacy, it does routinely have contact with foreign governments and foreign leaders on law enforcement issues. Matters pertaining to the enforcement of the laws of the United States and any foreign jurisdiction are by their very nature sensitive, and disclosure of information concerning these matters will often result in injury to the relationship that exists between the United States and a foreign nation, even years after the information was created. Accordingly, declassification reviewers must closely examine all FGI and information that pertains to a foreign government to determine whether it meets the “seriously and demonstrably” impair relations test outlined in Section 3.3(b)(6) of Executive Order 13526 for exemption from automatic declassification. In making this determination, declassification reviewers must also consider the nature of the information, the relationship between the United States and the foreign jurisdiction, promises of confidentiality extended to the foreign jurisdiction, the foreign jurisdiction’s policy on the disclosure of the information, age of the information, and the potential for harm to diplomatic activities and law enforcement cooperation.

(U) Information concerning foreign leaders and governments is commonly found in DOJ records. For the most part, the foreign government and foreign relations information appearing in these records concerns bilateral or multilateral efforts at cooperation against crime, particularly against illegal drugs and organized crime. Such records often contain blunt assessments of the commitment of foreign leaders and governments with regard to fighting crime and the illegal drug trade. It is not unusual for the Attorney General to travel and meet directly with foreign leaders. Background information for such visits, including foreign leader personality assessments and country reports, often appear in DOJ files. Such

U.S. Department of Justice
 Justice Management Division
 Security and Emergency Planning Staff

background information and after-action reports may contain foreign government information that could reasonably be expected to have an impact on the foreign relations of the United States. Additionally, it is possible that foreign government or foreign relations type information may have been distributed as part of the background information provided before or after NSC meetings attended by the Attorney General or his staff. Information that originated within DOJ that could reasonably be expected to 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 shall be exempted from automatic declassification.

(U) The passage of time, even 25-years, does not necessarily lessen the foreign relations impact that the declassification of foreign government/foreign relations related information may have. Leaders of many countries may be in power for decades and persons with whom the Department may have had sensitive meetings decades ago may just now be reaching the highest levels of their governments, which adds to the potential for foreign relation harm of information that may be decades old. Further, in the case of countries that do not maintain a close relationship with the United States, disclosure of law enforcement cooperation could become a source of much embarrassment for foreign leaders and result in refusal to cooperate in the future. Even among the close allies of the United States, law enforcement cooperation can be a sensitive subject for foreign leaders. When there is a doubt as to whether information requires continued protection under this exemption, the DOJ shall consult the Department of State (DOS) and, if necessary, the foreign government, to determine what damage may be caused to the foreign relations of the United States by the declassification of the information. If it is determined that information in DOJ records originated with another agency, DOJ will refer the information to the originating agency for final declassification review.

(U) NOTE: Declassification reviewers must consider the context and nature of information. Either favorable or unfavorable commentary in this category could originally have warranted classification. At 25 years, it is difficult to see how favorable commentary could be sufficiently damaging to warrant continued withholding unless it also suggested a controlling influence or overly deep involvement by the United States. The basic question is whether release of the information would seriously harm current U.S. diplomatic activities or impair relations. When the commentary is negative, the information is inherently more sensitive and more likely to require exemption from automatic declassification. Especially sensitive examples of negative commentary might include reports of corruption of individual officials, foreign government agencies, or other institutions, if the release of the information would impair current working relations.

TABLE 1.3 25X6 – FOREIGN RELATIONS (FOR)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as DOJ ADG 2.0 FOR-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
1	(U) Unless acknowledged, discussion of the benefits and risks of sharing information regarding a particular case with one or more particular foreign governments.	25X6	(U) This applies even after a decision to share.
2	(U) Identification of particular countries as eligible to receive more intelligence information than others.	25X6	(U) This applies whether it is a DOJ policy or a national policy.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.3 25X6 – FOREIGN RELATIONS (FOR)			
This table is UNCLASSIFIED//FOR OFFICIAL USE ONLY. Reference to an item from this table would be written as DOJ ADG 2.0 FOR-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
3	(U) Specific information about the extent of DOJ cooperation with a particular foreign government which would still cause harm to current relationships if revealed.	25X6	(U) This applies to cooperation on both criminal and national security cases. Information should be evaluated and researched to determine the level of acknowledgement of the cooperation. For example, DEA cooperation with foreign governments is widely acknowledged; however, specific details of that cooperation may require continued protection.
4	(U) Specific information about the extent of DOJ cooperation with a particular foreign government on a particular case which could still cause harm to current relationships if revealed.	25X6	(U) This applies to cooperation on both criminal and national security cases. Information should be evaluated and researched to determine the level of acknowledgement of the cooperation. Specific details of cooperation that have been revealed in court documents shall be declassified.
5	(U) Information received from a foreign government, which the originating government has marked as classified. All FGI should be evaluated for release or exemption in light of the originating country’s own policy on the release of its information.	25X6	(U) The DOJ routinely receives information from Foreign Governments that is marked “classified” but contains NO national security information. Information that is <u>clearly not national security information</u> should not be considered for exemption, regardless of its classification marking.
6	(U) Information provided by a foreign government which the originating government has indicated is classified, but which carries no classification markings. All FGI should be evaluated for release or exemption in light of the originating country’s own policy on the release of its information.	25X6	(U) The DOJ routinely receives information from Foreign Governments that contains NO national security information. Information that is clearly not national security information should not be considered for exemption.
7	(U) Specific details concerning the criteria and approval process for opening an investigation on foreign territory (extraterritorial investigation).	25X6	
8	(U) Specific details concerning the criteria and approval process for opening an investigation on U.S. territory in response to a request from a foreign government.	25X6	

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.3 25X6 – FOREIGN RELATIONS (FOR)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as DOJ ADG 2.0 FOR-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
9	(U) Information generated in an unacknowledged joint effort of the U.S. and one or more foreign governments that could harm or impair future cooperation if divulged.	25X6	(U) Provided there is an agreement among the participants regarding the level of protection for such information. (U) When there is no agreement on classification, but when an inference could reasonably be drawn regarding the cooperative relationship.
10	(U) Identification of a specific individual or organization as the subject of an espionage investigation-whether it is a threat assessment, a preliminary investigation, or a full investigation.	25X6	(U) Unless the individual or organization was publicly acknowledged and/or criminally prosecuted. Specific details may still be classified.
11	(U) Information which would enable an inference identifying a specific individual or organization as the subject of an espionage investigation-whether it is a threat assessment, a preliminary investigation, or a full investigation.	25X6	(U) Unless the individual or organization was publicly acknowledged and/or criminally prosecuted. Specific details may still be classified.
12	(U) Unless acknowledged, internal DOJ discussion about whether to open or close a particular investigation related to proliferation, infrastructure protection, or other foreign intelligence or foreign counterintelligence matters other than terrorism or espionage that could harm or impair current foreign relations.	25X6	(U) Specific details may still be classified even if officially acknowledged and/or criminally prosecuted.
13	(U) Identification of the subject of an espionage investigation that was carried out in cooperation with one or more foreign governments.	25X6	(U) Unless the individual or organization was publicly acknowledged and/or criminally prosecuted. Specific details may still be classified.
14	(U) Information concerning foreign political, economic, scientific, technical, social, military and cultural personalities, where this indicates that they have been, are currently or might become the targets of national security investigations pursuant to the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.	25X6	
15	(U) Information concerning closed unsolved espionage cases which were opened after the passage of the National Security Act of 1947 that could cause serious harm or impair current foreign relations.	25X6	(U) When in doubt if it could cause serious harm, refer to the State Department.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.3 25X6 – FOREIGN RELATIONS (FOR)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as DOJ ADG 2.0 FOR-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
16	(U) Identification of a specific individual or organization as the subject of a national security investigation related to proliferation, infrastructure protection, or other foreign intelligence or foreign counterintelligence matters other than terrorism or espionage-whether it is a threat assessment, a preliminary investigation, or a full investigation.	25X6	(U) Unless the individual or organization was publicly acknowledged and/or criminally prosecuted. Specific details may still be classified.
17	(U) Information which would enable an inference identifying a specific individual or organization as the subject of a national security investigation related to proliferation, infrastructure protection, or other foreign intelligence or foreign counterintelligence matters other than terrorism or espionage-whether it is a threat assessment, a preliminary investigation, or a full investigation.	25X6	(U) Unless the individual or organization was publicly acknowledged and/or criminally prosecuted. Specific details may still be classified.
18	(U) Identification of the subject of a national security investigation related to proliferation, infrastructure protection, or other foreign intelligence or foreign counterintelligence matters other than terrorism or espionage, when that investigation was carried out in cooperation with one or more foreign governments, and if divulged could harm or impair future cooperation.	25X6	
19	(U) Positive results or findings of a foreign threat assessment, preliminary investigation, or full investigation dealing with a national security threat other than international terrorism.	25X6	
20	(U) Information provided directly from a foreign leader or source as a result of cooperation on law enforcement matters or during diplomatic visits with foreign officials that could harm or impair current relations.	25X6	
21	(U) Minutes of meetings with foreign leaders or assessments of those meetings that could harm or impair current relations.	25X6	
22	(U) Assessments of foreign government commitment or ability to combat crime or the illegal drug trade in a manner consistent with United States' strategic goals in such policy areas.	25X6	
23	(U) Candid appraisals of foreign leaders or foreign organizations, including their personalities, or whether certain individuals or organizations may be corrupted by criminal organizations or drugs, among other things.	25X6	

U.S. Department of Justice
Justice Management Division
Security and Emergency Planning Staff

TABLE 1.3 25X6 – FOREIGN RELATIONS (FOR)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as DOJ ADG 2.0 FOR-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
24	(U) Evidence of foreign law enforcement cooperation with the United States under circumstances where the foreign government either requests that the cooperation be kept confidential, under circumstances where such an expectation can reasonably be inferred, and when release would cause serious harm to current U.S. diplomatic relations.	25X6	

(U) Other categories of foreign government information shall be referred to the State Department.

(U) 25X7 - PROTECTION OF THE PRESIDENT AND OTHER OFFICIALS

E.O. 13526, Section 3.3(b)(7): "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 the national security are authorized."

(U) This category of information should be used to continue classification protection of information that might be useful to individuals or organizations with the intent to harm U.S. or other persons authorized for protection. The Attorney General and certain other senior leaders of the DOJ are protected by a security detail of Special Agents authorized to provide for their safety and employed by component law enforcement offices. Because protection plans ordinarily are based upon plans used in the past and because the protection services are provided by Special Agents employed by the law enforcement components, specific information concerning the security provided to the Attorney General or other DOJ protectees could be exploited by terrorist groups or hostile foreign powers in such a way as to endanger the lives of the Attorney General and other DOJ protectees. Experience to date has shown that a limited amount of specific information regarding this security detail can appear in DOJ records and a small amount will be exempt from automatic declassification.

(U) When information described above has been originated by or involves another agency, the material should be referred to that agency for decision in accordance with section 3.3(d)(3) of E.O. 13526. For example: information about Secret Service protection should be referred to the Department of Homeland Security (DHS) for the Secret Service. Classified information in this category that applies only to a particular time or event, such as a schedule for a visit by the AG, or that relates to equipment, techniques, or practices that are no longer used or that are well known to the public, should not be exempted from declassification.

U.S. Department of Justice
 Justice Management Division
 Security and Emergency Planning Staff

TABLE 1.4 25X7 - PROTECTION			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 PRO-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
1	Procedures for conducting security surveys and protective security research that are still actively used.	25X7	
2	Relocation site surveys and locations while the sites remain in use for relocation.	25X7	
3	Information that describes travel protocols, tactics and procedures of a protective detail still in use.	25X7	

(U) 25X8 – EMERGENCY PREPAREDNESS & VULNERABILITIES OF INSTALLATIONS AND INFRASTRUCTURE

E.O. 13526, Section 3.3(b)(8): “Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.”

(U) In the event of a significant national emergency, plans have historically been, and currently are, in place to make sure that a cadre of DOJ officials are relocated to secure facilities so that they can continue the functions of the Department and support the President during such emergencies. Such plans are often referred to as Continuity of Government (COG) or Continuity of Operations (COOP) plans. Such plans appear in DOJ records and they contain details such as the identification of members of the DOJ cadre, the functions the cadre will perform in the event of a national emergency, gathering/meeting places to rendezvous with secure transportation, the mode of transportation to alternate sites, the names and locations of such sites, and types of secure communication equipment and codes.

(U) Also found among these types of records are exercise plans and scenarios used to test the COG/COOP plans. After action assessments of such exercises, which describe problems with or vulnerabilities within COG/COOP planning, also sometimes are located among these records. Beyond the immediate emergency scenario, there may also be information concerning the re-constitution of federal authority in the aftermath of a nuclear attack or other major disaster. Such plans and the exercise of the plans necessarily involve the information from a multitude of other federal agencies, including the Department of Defense (DoD) and the Federal Emergency Management Agency (FEMA) within the Department of Homeland Security (DHS). The declassification and disclosure of such information could reveal to terrorist groups and hostile foreign powers vulnerabilities in COG/COOP planning and could provide a roadmap for debilitating the United States government as a prelude to, or during, an attack on the United States. If in doubt about the current sensitivity of this type of information, DOJ declassification reviewers are instructed to consult the Continuity Assurance Section and/or refer it to FEMA, OSD, and/or the NSC if it involved COG in accordance with section 3.3(d)(3) of E.O. 13526.

(U) In the current era of international terrorism, there is a heightened awareness of the need to avoid dissemination of information relating to installations and infrastructure if it could be useful to individuals or organizations that might seek to harm U.S. facilities or persons. Much of that information, however, has not previously carried a security classification, but has been marked “Limited Official Use” (LOU) or “Sensitive But Unclassified” (SBU). When this material is reviewed, if it retains the potential to reveal continuing vulnerabilities, it should be classified CONFIDENTIAL and withheld under 25X8. Architectural plans of official installations still in use are an important example of heretofore

U.S. Department of Justice
 Justice Management Division
 Security and Emergency Planning Staff

unclassified documents that may need to be classified and withheld. This exemption should also be used to protect overseas emergency and evacuation plans and security surveys revealing vulnerabilities that could be utilized by terrorists. DOJ declassification reviewers should consult the DOJ National Security Information Classification Guide or other relevant guides for current guidance.

TABLE 1.5			
25X8 – EMERGENCY PREPAREDNESS & VULNERABILITIES			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 EPV-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
1	Information on the structure, design and layout of U.S. Government facilities, when that information is currently accurate and would facilitate hostile penetration or expose vulnerabilities.	25X8	
3	Security surveys including information revealing current vulnerabilities and mitigating countermeasures.	25X8	
4	Details about security, anti-sabotage or antiterrorism equipment or techniques that are still current or that expose vulnerabilities that would be useful to hostile elements planning an attack.	25X8	
5	Information detailing emergency relocation plans, techniques and/or procedures, and Continuity of Government and Continuity of Operations plans that are still in use; including facilities and locations.	25X8	
6	Information concerning security alarms, monitoring devices and other systems for protection against physical penetration or attack when they are current or when the information would create vulnerability in current systems.	25X8	
7	Information that would reveal the current security procedures, staffing, tactics, weapons, equipment, procedures or protocols for the protection of DOJ employees and any DOJ facility.	25X8	
8	Information that would reveal the current security procedures, staffing, tactics, weapons, equipment, procedures or protocols for the protection of DOJ communications or information processing systems.	25X8	

(U) 25X9 – STATUTES, TREATIES, OR INTERNATIONAL AGREEMENTS

E.O. 13526, Section 3.3(b)(9): “Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.”

(U) DOJ will rarely, if ever, exempt information from automatic declassification under this exemption. Further, this type of exemption refers **only** to information collected under a statute, treaty, or agreement categorized as *classified national security information*. This does not apply to the broader universe of all information the release of which is limited by statute, treaty or agreement.

(U) The United States has entered into agreements with a number of other countries that provide for the protection of classified information. When they are government-to-government agreements, they are generally called General Security of Information Agreements (GSOIA’s). More common are General Security of Military Information Agreements (GSOMIA’s) which, as the name implies, are military-to-military agreements. Such agreements specify the conditions under which information originated by the parties may be released to other parties or the public. Where such agreements exist, the USG is bound by them.

U.S. Department of Justice
 Justice Management Division
 Security and Emergency Planning Staff

(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.

TABLE 1.6 25X – STATUTES, TREATIES, OR INTERNATIONAL AGREEMENTS (STAT)			
This table is UNCLASSIFIED// FOR OFFICIAL USE ONLY . Reference to an item from this table would be written as: DOJ ADG 2.0 STAT-item #			
ITEM #	DESCRIPTION	EXEMPT/ REDACT	COMMENTS
1	(U) Information, the release of which would violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.	25X9	Documents marked as exempt from declassification for this reason must identify the statute, treaty or other international agreement. Reviewers must consult internally prior to applying this exemption to ensure the proper interpretation of the statute, treaty, or agreement in question.
2	(U) Information collected pursuant to a statute which requires classification.	25X9	Documents marked as exempt from declassification for this reason must identify the specific section of the U.S. code requiring their classification.

(U) FURTHER EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION AT 50 YEARS

Executive Order 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 could 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."*

(U) With the exception of the FBI, the DOJ does not have any "extraordinary case" 50X exemptions and does not anticipate a future need within the next 5 years.