

RELEASE IN PART
B7(C),B6

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between

Hillary Rodham Clinton

and the United States.

(Name - Printed or Typed)

REVIEW
AUTHORITY:
Barbara
Nielsen,
Senior
Reviewer

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in the Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods, and is classified or is in process of a classification determination under the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI. I further understand that I am obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to be submitted for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or showing it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable; If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

FORM
7-97

4414

(EF)

(Replaces Form 4355-
which is obsolete and
will not be used)FORM
7-97

4414

(EF)

Page 1 of 2

• B6

B6
B7(C)
B6
B7(C)

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

FORM 11-60 4414 (EF)

Page 2 of 2

22 January 2009
Date

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc No. C05833712 Date: 11/05/2015

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between Hillary Rodham Clinton and the United States.

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in the Agreement as Sensitive Compartmented Information (SCI), the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted to SCI, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized by access to SCI, whether or not I am still employed by or associate with that the Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI. I further understand that I am obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.
4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to be submitted for security review by the Department or Agency that last authorized by access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that any obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation wit, or showing it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.
5. I understand that the purpose of the review described in paragraph 4 is to give the United States a

reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in my termination of any access to SCI and removal from a position of special confidence and trust requiring such access as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Sections 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the actions can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose the action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provision of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952, Title 18, United States Code, and of Sections 783(b), Title 50, United States Code, and Executive Order

[TRANSCRIPTION]

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc. No. C05833712 Date: 11/05/2015

12958, as amended, so that I may read them at this time if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remuneration, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelations not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights [sic] or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosure to Congress); Section 10, United States Code, as amended by the Military Whistleblowers Protection Act (governing disclosures to Congress by members of the Military), Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (government disclosure of illegality, waste, fraud, abuse, or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.)(governing disclosures that could expose confidential Government agents), and the statute which protect agent disclosure which may compromise national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.

Signature: H.R. Clinton

Date: 22 January 2009

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE

Signature: [Signature redacted]

Date: 22 January 2009

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGEMENT

SI G TK HCS

SSN: (See Notice Below) [SSN number redacted]

Printed or Typed Name: Hillary Rodham Clinton

Organization: S

BRIEF

Date: 22 January 2009

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

[TRANSCRIPTION]

UNCLASSIFIED U.S. Department of State Case No. F-2015-05069 Doc. No. C05833712 Date: 11/05/2015

Signature: HR Clinton

DEBRIEF

Date: [Blank]

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on this above SCI Special Access Program(s):

Signature: [Blank]

I certify that the briefing presented by me on the above date was in accordance with the relevant SCI procedures

Signature of Briefing/Debriefing Officer: [Signature redacted]

SSN (See Notice Below): [SSN redacted]

Printed or Typed Name: [Redacted]

Organization (Name and Address): DS/IS/SSO State

NOTICE: The Privacy Act, 5 U.S. C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

FORM 11-0Q

4414

(EF)

FORM 7-97

4414

(EF) (Replaces Form 4355-which is obsolete and will not be used)

[REVIEWER ANNOTATIONS]

RELEASED IN PART B7(C),B6

REVIEW AUTHORITY: Barbara Nielsen, Senior Reviewer

B6

B7(C)

B6

B7(C)

B6

B7(C)

FOIA UPDATE: EXECUTIVE ORDER 12958--CLASSIFIED NATIONAL SECURITY INFORMATION

January 1, 1995

FOIA Update
Vol. XVI, No. 2
1995

EXECUTIVE ORDER 12958 -- CLASSIFIED NATIONAL SECURITY INFORMATION

The following is the text of Executive Order No. 12958--Classified National Security Information -- in an abridged form. This executive order was issued by President Clinton on April 17, 1995, and will take effect on October 14, 1995. It supersedes Executive Order No. 12,356, which was issued in 1982.

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open government.

Part 1--ORIGINAL CLASSIFICATION

* * * * *

Sec. 1.2. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
 - (2) the information is owned by, produced by or for, or is under the control of the United States Government;
 - (3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and
 - (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.
- (b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:
- (1) amplify or modify the substantive criteria or procedures for classification; or
 - (2) create any substantive or procedural rights subject to judicial review.
- (c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. Classification Levels. (a) Information may be classified at one of the following three levels:

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

* * * * *

Sec. 1.5. Classification Categories.

Information may not be considered for classification unless it concerns:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities; or
- (g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

- (b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.
- (c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.
- (d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security, for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

- (1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

- (2) reveal information that would assist in the development or use of weapons of mass destruction;
 - (3) reveal information that would impair the development or use of technology within a United States weapon system;
 - (4) reveal United States military plans, or national security emergency preparedness plans;
 - (5) reveal foreign government information;
 - (6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;
 - (7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
 - (8) violate a statute, treaty, or international agreement.
- (e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with Part 3 of this order.

Sec. 1.7. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

- (1) one of the three classification levels defined in section 1.3 of this order;
- (2) the identity, by name or personal identifier and position, of the original classification authority;
- (3) the agency and office of origin, if not otherwise evident;
- (4) declassification instructions, which shall indicate one of the following:
 - (A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or
 - (B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or
 - (C) the exemption category from declassification, as prescribed in section 1.6(d); and
- (5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

* * * * *

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

* * * * *

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified 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 national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information

* * * * *

Part 2--DERIVATIVE CLASSIFICATION

* * * * *

Sec. 2.2. Use of Derivative Classification. (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

- (1) has program or supervisory responsibility over the information or is the senior agency official; and
- (2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

* * * * *

Part 3--DECLASSIFICATION AND DOWNGRADING **Sec. 3.1. Definitions.** For purposes of this order:

* * * * *

(b) "Automatic declassification" means the declassification of information based solely upon:

- (1) The occurrence of a specific date or event as determined by the original classification authority; or
- (2) the expiration of a maximum time frame for duration of classification established under this order.

* * * * *

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.

* * * * *

Sec. 3.4. Automatic Declassification. (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

- (1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;
- (2) reveal information that would assist in the development or use of weapons of mass destruction;
- (3) reveal information that would impair U.S. cryptologic systems or activities;

- (4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;
- (5) reveal actual U.S. military war plans that remain in effect;
- (6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- (7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
- (8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
- (9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the file series;
- (2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

* * * * *

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

* * * * *

Sec. 3.5. Systematic Declassification Review. (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order.

* * * * *

Sec. 3.6. Mandatory Declassification Review. (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

- (1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;
- (2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

* * * * *

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

* * * * *

Sec. 3.7. *Processing Requests and Reviews.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. *Declassification Database.* (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

* * * * *

Part 5--IMPLEMENTATION AND REVIEW

* * * * *

Sec. 5.2. *Program Direction.* (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

- (1) classification and marking principles;
- (2) agency security education and training programs;
- (3) agency self-inspection programs; and
- (4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

* * * * *

Sec. 5.3. *Information Security Oversight Office.* (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

* * * * *

Sec. 5.4. *Interagency Security Classification Appeals Panel.*

(a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

* * * * *

(b) Functions. The Panel shall:

- (1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;
- (2) approve, deny or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and
- (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

* * * * *

Sec. 5.5. *Information Security Policy Advisory Council.*

(a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated interest and expertise in an area related to the subject

matter of this order and are not otherwise employees of the Federal Government.

* * * * *

(b) Functions. The Council shall:

- (1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;
- (2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and
- (3) serve as a forum to discuss policy issues in dispute.

* * * * *

Sec. 5.6. General Responsibilities. Heads of agencies that originate or handle classified information shall:

* * * * *

(c) designate a senior agency official to direct and administer the program whose responsibilities shall include:

* * * * *

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

* * * * *

Sec. 5.7. Sanctions.

* * * * *

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- (1) disclose to unauthorized persons information properly classified under this order or predecessor orders;
- (2) classify or continue the classification of information in violation of this order or any implementing directive;
- (3) create or continue a special access program contrary to the requirements of this order; or
- (4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

* * * * *

Part 6--GENERAL PROVISIONS

Sec. 6.1. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security

Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. *Effective Date.* This order shall become effective 180 days from the date of this order [October 14, 1995].

Go to: [FOIA Update Home Page](#)

Topic(s):

FOIA Update

Posted in:

[Office of Information Policy](#)

Updated August 13, 2014