E.O. 12958
03 17 April 1995

as authorized by the

activities that the IOB
or Presidential direc-

concerning intelligence
ary to Executive order

within the Intelligence
ivities;
tors General and Gen-
ig and reporting intel-
ecutive order or Presi-

essary to carry out its

port to the President
and take appropriate
ntral Intelligence, the
ice Community. With
IOB shall advise and
intelligence, the Cen-
Community.

elligence Community,
information that the
rs General and Gen-
rmitted by law, shall
to time as necessary
ive reason to believe
directive.

mbers of the PFIAB
rity protection in ac-
of the PFIAB, each
nts shall execute an
y virtue of his or her
ons as the President

nsation but may re-
orized by law. Staff
as authorized by the

s amended, and Ex-
voked.

LLIAM J. CLINTON

EXECUTIVE ORDER NO. 12958 CLASSIFIED NATIONAL SECURITY INFORMATION

(April 17, 1995, 76 F.R. 19825)

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.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

Section 1.1. *Definitions.* For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any military department; and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that 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.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

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.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuat to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original cla
tion as provided in
(e) Exceptional
or grantee of an a
nates information b
shall be protected i
rectives. The infor
order or its impleme
ter interest and cla
cy shall decide with
which agency has c
to the Director of th
termine the agency
mation, with approp
mination

Sec. 1.5. *Classif*
Information ma
(a) military plan
(b) foreign gover
(c) intelligence
methods, or cryptolo
(d) foreign relat
fidential sources;
(e) scientific, tec
rity;
(f) United State
facilities; or
(g) vulnerabiliti
lating to the nationa

Sec. 1.6. *Durati*
original classificatio
for declassification b
the information. The
(b), below.
(b) If the origina
date or event for de
10 years from the da
below.
(c) An original cl
or reclassify specific
time if such action
under this order. Th
that are more than 2
torical value under tit
(d) At the time of
exempt from declassif
disclosure of which c
security for a period
release of which could
(1) reveal an
or activity;
(2) reveal inf
ons of mass destr
(3) reveal inf
nology within a U
(4) reveal U
paredness plans
(5) reveal for
(6) damage
reveal
(7) impair
(8) violate a statut

nization that has pro-
rmation to the United
ie expectation that the
ce.
national defense or for-
closure of information,
).

be originally classified
ions are met:
ie information;
or is under the control

egories of information

hat the unauthorized
d to result in damage
hority is able to iden-

information, it shall

cedures for classifica-

to judicial review.
atically as a result of

assified at one of the

iauthorized disclosure
ally grave damage to
rity is able to identify

thorized disclosure of
ge to the national se-
identify or describe.
unauthorized disclo-
ge to the national se-
identify or describe.
ms shall be used to

el of classification, it

ify information origi-

ident in the Federal

authority pursuat to

ed level are also au-

ll be limited to the
are responsible for
nonstrable and con-

e delegated only by
rsuant to paragraph

hority may be dele-
gnated pursuant to
led that official has
by the agency head.
shall be in writing
ided in this order.
title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

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 weapons 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.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(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.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(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 it
be classified if the compi
tionship that:
(1) meets the sta
(2) is not otherwi
As used in this order, "c
fied items of information.

Sec. 1.9. *Classificati*
in good faith, believe tha
expected to challenge the
agency procedures establi
(b) In accordance wi
an agency head or senior
thorized holders of inform
fication of information t
These procedures shall as
(1) individuals ar
(2) an opportuni
and
(3) individuals a
Interagency Security
this order.

PART 2—DERIVATIVE

Sec. 2.1. *Definitions*
means the incorporating
mation that is already c
sistent with the classi
tion. Derivative classificat
sification guidance. The c
is not derivative classific
(b) "Classification gu
classification of specific i
(c) "Classification gu
issued by an original clas
tion regarding a specific
duration of classification
(d) "Source documen
formation that is incorpo
a new document.
(e) "Multiple source
guides, or a combination

Sec. 2.2. *Use of Der*
tract, or summarize class
derived from source mat
sess original classificatio
(b) Persons who appl
(1) observe and
(2) carry forwar
tion markings. For i
the derivative classif
(A) the date
period of classifi
(B) a listing
copy.

Sec. 2.3. *Classificat*
ity shall prepare classifi
classification of informa
directives issued under
(b) Each guide shal
(1) has program
senior agency officia
(2) is authorize
classification prescri
(c) Agencies shall e
reviewed and updated as

classification under prede-
nation Required," or infor-
no declassification instruc-
; order.

e of original classification,
document, or shall be ap-

n section 1.3 of this order;
nd position, of the original

: evident;
ıte one of the following:
)rescribed in section 1.6(a)

f original classification, as

tion, as prescribed in sec-

minimum, cites the appli-
er
ıbove, may be excluded if

ıer means, indicate which
vel, which portions are ex-
:r, and which portions are
irectives issued under this
Office may grant waivers
information. The Director

r, including abbreviations
rs, shall conform to the
rsuant to this order.
iginal classification mark-
les a degree of protection
ırnished the information.
this or predecessor orders
tion despite the omission
is used in the derivative
:ation, holders of such in-
)n authority for the appli-

:able, use a classified ad-
ll portion of an otherwise

a) In no case shall infor-

strative error;
)n, or agency;

t does not require protec-

ated to the national secu-

)een declassified and re-

to the public under prop-
:y has received a request
2) or the Privacy Act of
f section 3.6 of this order
rder and is accomplished
:ipation or under the di-
enior agency official des-
s not apply to classified
rs old and have been de-
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 in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2—DERIVATIVE CLASSIFICATION

Sec. 2.1. *Definitions.* For purposes of this order: (a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

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.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. DEFINITIONS. For purposes of this order: (a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(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.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(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.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. *Transferred Information.* (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in posses-

sion after consultation wi
matter of the information.

(c) Classified informat
Administration ("National
declassified or downgraded
tives issued pursuant to tl
procedural agreement betw

(d) The originating ag
information contained in r
fore they are accessioned
require that records conta
tional Archives when nece
Act. This provision does n
pursuant to section 2203
the National Archives an
records of an agency or org

(e) To the extent prac
ment that will facilitate th
are declassified pursuant
1.6 and 3.4 of this order.

Sec. 3.4. *Automatic D*
5 years from the date of
that (1) are more than 25
nent historical value unde
classified whether or not
fied information in such r
25 years from the date of
(b), below.

(b) An agency head r
graph (a), above, specific

(1) reveal the ider
about the application
of a human intelligen
would clearly and de
United States;

(2) reveal informa
ons of mass destructio

(3) reveal informa
ties;

(4) reveal informa
technology within a U

(5) reveal actual I

(6) reveal informa
tions between the Uni
monstrably undermine

(7) reveal informa
rent ability of United
President, and other c
tional security, are au

(8) reveal informa
rent national security

(9) violate a statu

(c) No later than the
the President through the
of any specific file series o
that the information with
more of the exemption cat
cy proposes to exempt fror

(1) a description

(2) an explanatio
invariably exempt fr
must remain classifie

(3) except for the
ligence source, as pr
declassification of
not to exempt the
at an earlier date tha

GRADING

order: (a) "Declassification" means
n from classified information to un

eclassification of information based

vent as determined by the original

frame for duration of classification

inal classification, if that official is

unction.

uthority in writing by the agency

ns the review for declassification of
r declassification that meets the re-

is the review for declassification of
lave been determined by the Archi-
rmanent historical value in accord-
ode.

structions issued by a declassifica-
rmation regarding a specific subject
ust remain classified.

oy a declassification authority that
ecified level shall be classified and

il, regardless of its physical form or
with a filing system or maintained
or activity.

information shall be declassified as
sification under this order.

tinues to meet the classification re-
ed protection. In some exceptional
tion may be outweighed by the pub-
nd in these cases the information
rise, they shall be referred to the
fficial will determine, as an exercise
losure outweighs the damage to na-
ted from disclosure. This provision

criteria or procedures for classifica-

rights subject to judicial review.

ty Oversight Office determines that
r, the Director may require the in-
t originated the classification. Any
o the President through the Assist-
airs. The information shall remain
al.

apply to agencies that, under the
ication authority, but had such au-

the case of classified information
nctions, and not merely for storage
be the originating agency for pur-

is not officially transferred as de-
ated in an agency that has ceased
gency, each agency in possession of
inating agency for purposes of this
owngraded by the agency in posses-

sion after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

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.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and 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 Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

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

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

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. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist of the shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

773

Sec. 3.6. *Ma*
graph (b), below,
shall be subject to
(1) the re
the informati
a reasonable
(2) the in
tral Intelligen
(3) the ir
past 2 years.
years, or the
inform the re
(b) Informatic
(1) the in
(2) the in
(3) comm
dent; or
(4) other
vise and assi
paragraph (a)
downgrade, a
of the Archivi
United States
for consultati
be consistent
pertain to th
subject matte
Any final de
agency to the
tion shall ren
(c) Agencies
information that
They shall releas
warranted under
(d) In accord
shall develop pro
information. Thes
predecessor order
a denial of a man
to appeal a final
Panel.
(e) After cons
velop special pro
Central Intelliger
pertaining to int
sources or metho
view of informatic

Sec. 3.7. *Pro*
tion under the Fr
tory review provi
or systematic revi
(a) An agenc
requested inform
classified under t
(b) When an
tain information
such documents
provisions of this
ments to the orig
originating agenc
itself classified u
mines in writing
ring agency shall

Sec. 3.8. *De*
Director of the In
nate classified inf

matically declassified under this
all notify the Director of the In-
ecutive Secretary of the Inter-
ny specific information beyond
r paragraph (c), above, that the
cation. The notification shall in-

s exempt from automatic declas-
r period of time; and
human source or a human intel-
ove, a specific date or event for
nay direct the agency not to ex-
earlier date than recommended.
o the President through the As-
Affairs. The information will re-

der, the agency head or senior
ormation Security Oversight Of-
nts of this section, including the
an shall include the requirement
e records affected by this section
order, and similar commitments
matic declassification.
classification under this section
itic declassification review provi-

n the United States should com-
f a foreign government or inter-
y treaty or international agree-
contained in records affected by
the date of its creation, unless
information that may otherwise
.

(a) Each agency that has origi-
predecessors shall establish and
eview. This program shall apply
matic declassification under sec-
he systematic review of records

Security Policy Advisory Council,
cific subject areas for systematic

the likelihood of declassification

matic declassification review pro-
o the National Archives as of the
rred to the Archivist pursuant to
3) information for which the Na-
s as the custodian of the records
of existence. This program shall
from the date of their creation.
stematic review of these records
n Security Policy Advisory Coun-
ikelihood of declassification upon
dance with the standards of this
tion guides provided to the Archi-
e Director of the Information Se-
s provide the Archivist with ade-

the Secretary of Defense may es-
for declassification of classified
al Intelligence may establish spe-
ification of classified information
special activities), or intelligence

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.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

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 informa-

tion that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4—SAFEGUARDING

Sec. 4.1. *Definitions.* For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. *General Restrictions on Access.* (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside

any other agency to which
originating agency. An agen
ment for specific information
tion, the Department of Defe

Sec. 4.3. *Distribution C*
distribution of classified info
tions or individuals eligible
tion.

(b) Each agency shall u
curring distribution of class
cooperate fully with distribu
distributors whenever a rele

Sec. 4.4. *Special Access*
Unless otherwise authorized
and Energy, and the Direc
each, may create a special
to intelligence activities (incl
ational, strategic and tactic
function will be exercised
shall keep the number of th
lish them only upon a specifi

(1) the vulnerability

(2) the normal crite
formation classified at
information from unauth

(3) the program is r

(b) *Requirements and Li*

(1) Special access p
ber of persons who will
mensurate with the obj
tion involved.

(2) Each agency he
for special access progr
order.

(3) Special access p
lished under section 5.6(
tion Security Oversight
cordance with the secur
the functions assigned t
order. An agency head
rector and no more thar
sight Office; or, for spe
and vulnerable, to the D

(4) The agency head
access program to deter
this order.

(5) Upon request, a
National Security Affai
special access programs.

(c) Within 180 days aft
principal deputy shall revie
jurisdiction. These officials
clearly meet the provisions
an agency head or principa
lished on the effective date o

(d) Nothing in this ord
10 U.S.C. 119.

Sec. 4.5. *Access by Hist*
(a) The requirement in sect
mation may be granted only
may be waived for persons w

(1) are engaged in h

(2) previously have
pointed by the President

(b) Waivers under this s
agency official of the origina

any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. *Distribution Controls.* (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. *Special Access Programs.* (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) *Requirements and Limitations.*

(1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. *Access by Historical Researchers and Former Presidential Appointees.* (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. *Definitions.* For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

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.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

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.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director ofthe Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for or
cials not granted original cl
recommend Presidential appr
ment and Budget;

(6) consider and take ac
within or outside the Governi
gram established under this c

(7) have the authority t
cies, standardization of forms
tion of the program establishe

(8) report at least annua
order; and

(9) convene and chair in
to the program established by

Sec. 5.4. *Interagency Securit*
and Administration.

(1) There is established
Panel ("Panel"). The Secretar
Director of Central Intelligen
sistant to the President for N
level representative to serve
lect the Chair of the Panel fr

(2) A vacancy on the Pan
in paragraph (1), above.

(3) The Director of the Ir
the Executive Secretary. The
shall provide program and ad

(4) The members and sta
for access standards in order

(5) The Panel shall meet
meetings as may be necessa
manner.

(6) The Information Secu
the President a summary of t

(b) *Functions.* The Panel shal

(1) decide on appeals by
under section 1.9 of this orde

(2) approve, deny, or ame
tion as provided in section 3.

(3) decide on appeals by
mandatory declassification re

(c) *Rules and Procedures.* Tl
lished in the Federal Register no
order. The bylaws shall establish
in accepting, considering, and is
dures of the Panel shall provide t
in which:

(1) the appellant has exh
the responsible agency;

(2) there is no current ac
and

(3) the information has r
or the Panel within the past

(d) Agency heads will coope
functions in a timely and fully in
cision of the Panel to the Presid
tional Security Affairs.The Panel
to the President for National Sec
an agency head is not cooperatin

(e) The Appeals Panel is esta
ng the President in the dischar
to protect the national security o
to the discretion of the Panel, uni

Sec. 5.5. *Information Securit*
is established an Information S
Council shall be composed of se
gered terms not to exceed 4 year

is consistent with the interest of na-

classified information from unauthor-
s that the information is safeguarded
id
Presidential appointees to items that
or received while serving as a Presi-

EW

order: (a) "Self-inspection" means the
agency activities and the agency as a
f the program established under this

tion that could reasonably be expected
sified information;
action to classify or continue the clas-
equirements of this order or its imple-

t action to create or continue a special
nts of this order.
ful, or negligent action contrary to the
ng directives that does not comprise a

ector of the Office of Management and
the President for National Security Af-
y Board, shall issue such directives as
e directives shall be binding upon the
f the Office of Management and Budget

ples;
aining programs;
and
guides.
ment and Budget shall delegate the im-
is program to the Director of the Infor-

ed by a Presidential Decision Directive,
ent through the Assistant to the Presi-
ect to the issuance of a Presidential di-
n. The Presidential directive shall per-
transmittal, and destruction of and ac-

t Office. (a) There is established within
formation Security Oversight Office. The
Budget shall appoint the Director of the
ct to the approval of the President.
f the Office of Management and Budget
the President for National Security Af-
ty Oversight Office shall:
nentation of this order;
e compliance with this order and its im-

lementing regulations and agency guides
ior to their issuance by the agency;
n-site reviews of each agency's program
quire of each agency those reports, infor-
y be necessary to fulfill its responsibil-
tegories of classified information would
isk, the affected agency head or the sen-
n justification recommending the denial
Management and Budget within 60 days
be denied pending a prompt decision by
nt and Budget, who shall consult on this
dent for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

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.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(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.

(c) *Rules and Procedures.* The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the federal courts; and

(3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs.The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

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 in

terest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C.App. 2.

(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 policiesestablished 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.

(c) *Meetings.* The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) *Administration.*

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. *General Responsibilities.* Heads of agencies that originate or handle classified information shall: (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order; (b) commit necessary resources to the effective implementation of the program established under this order; and (c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programsauthorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access toclassified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(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; (8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the

Information Securit
prompt manner age
complaint, or sugge
formation that origi
and for which there

Sec. 5.7. *Sanctions.*
fice finds that a violatio
curred, the Director shal
agency official so that cor
(b) Officers and emp
tors, licensees, certificate
tions if they knowingly, w
(1) disclose to ur
this order or predeces
(2) classify or cor
order or any impleme
(3) create or conti
of this order; or
(4) contravene an
tives.
(c) Sanctions may inc
nation of classification au
or other sanctions in accor
(d) The agency head,
at a minimum, promptly r
demonstrates reckless disr
standards of this order.
(e) The agency head or
(1) take appropriat
fraction under paragrap
(2) notify the Direc
violation under paragra

PART 6 GENERAL—PRO

Sec. 6.1. *General Provis*
quirement made by or unde
National Security Act of 19
stricted Data" shall be hand
in conformity with the prov
and regulations issued under
(b) The Attorney General
of the Information Security
order with respect to any que
(c) Nothing in this order
provisions of law, including t
Privacy Act, and the Nationa
intended, and should not be
or procedural, enforceable at
its officers, or its employees.
forth in sections 1.2(b), 3.2(b)
(d) Executive Order No
date of this order.

Sec. 6.2. *Effective Dat*
date of this order

matter of this order and are
The President shall appoint
il shall comply with the Fed-
2

President for National Secu-
nt and Budget, or such other
on policiesestablished under
ıg recommended changes to

for specific subject areas for

ispute.
each calendar year, and as
onal Security Affairs or the

at a rate of pay not to ex-
pay in effect for grade GS-
itle 5, United States Code,
l in the actual performance

ce of business in the actual
may be allowed travel ex-
s authorized by law for per-
e (5 U.S.C. 5703(b)).
to the availability of funds,
ide the Council with admin-
t services necessary for the

the functions of the Presi-
amended, that are applica-
ongress, shall be performed
ıt Office in accordance with
eneral Services Administra-

es that originate or handle
mmitment and commit sen-
program established under
tive implementation of the
a senior agency official to
s shall include:
under this order, provided,
to oversee special access
hall provide a full account-
nnually;
h shall be published in the
ers of the public;
ion and training programs;
-inspection program, which
he agency's classified prod-

y access to classified infor-
need for access toclassified
ative clearance procedures;
ccess to classified informa-
ıonal and security require-

safeguarding of classified
ile areas;
ıer system used to rate c-
management of classified
uated in the rating of: (i)
ers or security specialists;
ly involve the creation or
the costs associated with
rted to the Director of the

Information Security Oversight Office for publication; and(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(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.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

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.

WILLIAM J. CLINTON