GINA to FAXED

Jan. 23, 1995

To: Bob Damus

From: Doug Letter

Re: Comments Regarding Proposed Executive Order Regarding Classified Information

As I mentioned to you on the phone, Judge Mikva and I went over the proposed order and had some questions and comments, which are set out below. After you have had a chance to look at them, let me know (456-7901) so that I can stop by to discuss. Thank you.

A. At two points (Sec. 1.2(b) and 3.2(b)), the Order says that a particular provision does not create substantive or procedural rights subject to judicial review. This specificity makes it seem that other parts of the Order might indeed create such rights. We do not understand this to be the intent of the Order. It would therefore seem to make more sense to add a separate overall provision in Part 6 -- which contains the General Provisions -- saying something like: "Nothing in this Order is meant to create any substantive or procedural rights, and nothing in this Order is meant to be the subject of judicial review."

These same two sections contain the clause that these provisions do not "Amplify or modify the substantive criteria or procedures for classification." We find this sentence confusing, and it does not seem to add anything to the otherwise clear provision in Section 1.2(b) to the effect that officials with classification authority should lean against classification if there is a close call. We would delete the added disclaimer as unhelpful.

B. There appears to be a problem with the definition of "Agency" in Sec. 1.1(i), which merely refers to 5 U.S.C. § 552(f). This is the FOIA definition of "agency," which, under current FOIA case law, would not cover some parts of the White House, including entities such as the White House Counsel's Office. (And, is the NSC an agency under the FOIA definition? See discussion below.) Yet, we believe that the President wants this Order to cover all parts of the White House too. So, this definition of "agency" should be broadened.

C. Section 1.8(a)(2) says that information should not be classified in order to "prevent embarrassment to a person, organization, or agency." Does this make sense if the information involves a foreign personage? If we have embarrassing information about a current foreign head of state (for example, the Emperor of Japan), we assume that is something that might legitimately be classified, even if the same

information about our own Government officials should properly be disclosable.

D. Section 1.8(c) says that information may not be reclassified after it has been declassified and released to the public under proper authority. We agree with this point in general; one administration should not attempt to reclassify material that has been declassified by a prior one. However, the order should be phrased to take account of the unusual circumstance in which a mistake has simply been made. See, e.g., the factual situation described in American Library Assn. v. Faurer, 631 F. Supp. 416 (D.D.C. 1986) and American Library Assn. v. Odom, 818 F.2d 81 (D.C. Cir. 1987). There, sensitive cryptographic information had been declassified by mistake (but by the "proper authority") and placed on the shelves in a library that was open to the public. When the mistake was discovered, the agency reclassified it. This would seem to be a legitimate action, but the current draft would appear to prohibit that appropriate remedial action in the future.

E. Section 3.4(b)(2) allows exemption from automatic declassification for information whose release would "reveal information that would impair United States cryptographic systems or activities." Our understanding is that the United States is so far ahead of much of the rest of the world in this area that cryptographic technology we used many years ago and that is not of value to us any more, could still be useful to underdeveloped countries. We likely do not want to provide aid inadvertently to other countries so that they can better encrypt information. We would suggest changing this to read: "* * * reveal information that would impair United States cryptologic systems or activities, or aid such systems or activities in other countries."

F. Section 3.6(c) provides that declassified information shall be released "unless withholding is otherwise authorized and necessary under applicable law." We think this is not worded correctly. Some information might be declassified, but still covered by privileges, such as the deliberative process privilege. Withholding of such material is "authorized" by the FOIA, but is not "necessary" under that statute; in general, withholding under the FOIA exemptions is not necessary, but is discretionary. This proposed provision would seem to make more sense if phrased as: "unless withholding is otherwise authorized and warranted [or "appropriate"] under applicable law."

This same concern is raised by Sec. 3.8(c), which allows for withholding "as otherwise provided by law." Given the discretionary nature of the FOIA disclosure exemptions, a better operative phrase would seem to be "as otherwise authorized by law."

Also note that these provisions do not seem fully consistent with Sec. 6.1(c), which states that nothing in this Order "limits the protection afforded any information by other provisions of law * * *." This final overall provision does not speak of protecting information if withholding is "necessary." If the provisions discussed above are changed as we suggest, this inconsistency seems to disappear. We would also change the wording of Sec. 6.1(c) to: "Nothing in this Order limits the protection afforded any information by other provisions of law, including but not limited to the exemptions in the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947."

G. Section 5.4(b) provides for appeals to the Interagency Security Classification Appeals Panel, and decisions by that group. Shouldn't the Order state how that group is to decide such appeals, i.e., by majority vote, or otherwise? And, if the concerned agency head feels strongly enough, can he/she take the issue to the White House and get a reversal of the Appeals Panel decision? We assume so; shouldn't it be clear that the President retains authority to override the Panel? (See Sec. 3.4(d)(3), which provides specifically for such an appeal in some instances.)

Also with regard to this panel, should there be a representative from the Department of Energy, since that office possesses much classified nuclear weapons information? (Note the inclusion of the Secretary of Energy in Sec. 4.4.)

H. There is a controversy brewing -- in district court, we think -- about whether the NSC is a FOIA agency. This question turns in part on whether the NSC has power independent of the President, or just serves as his arm. This proposed Order in several places (e.g., Sec. 3.2(c), 5.2(a), 5.3(b)) gives the NSC some independent power, and that action could undermine any attempt to argue that the NSC is not a FOIA entity. At some points (see Sec. 3.4(d)(3)), the Order makes clear that the NSC is acting for the President. We would make this clear in the other sections as well, saying something like: "The NSC, acting as the agent of the President * * *," or "The President, through the NSC, shall * * *."

I. There are a few instances of what seem to be simple drafting mistakes:

Sec. 3.1(c)(1) should possibly end with "* * * is still serving in the same or an equivalent position."

Sec. 3.4(d) begins: "At least 180 days before it becomes subject to automatic declassification * * *." It is not clear what the "it" refers to; it seems to refer to the agency head,

but we assume it was meant to refer instead to information. Something needs to be reworded here.

Sec. 3.6(a)(1) begins: "The request describes * * *." Neither this provision nor the beginning of the section says what request this provisions covers. If this is fixed, that should solve a similar problem in subsection (3).

Sec. 4.4(a) lists several agencies having classified information; does the Nuclear Regulatory Commission have such information? Should it be included?

Sec. 5.5(a) establishes the Information Security Policy Advisory Council by stating: "The Council shall be comprised of seven members * * *." For correct phrasing, this should read: "The Council shall be composed of * * *," or "The Council comprises * * *."

Sec. 5.5(d)(4) is quite confusing and we cannot figure out what it means. It would appear to need rewriting.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

March 30, 1995

95 MAR 31 P12 : 43

MEMORANDUM FOR DESIGNATED AGENCY HEADS
(SEE ATTACHED DISTRIBUTION LIST)

FROM: Robert G. Damus RGD
General Counsel

SUBJECT: Proposed Executive Order Entitled "Access to Classified Information"

Attached is a proposed Executive order entitled "Access to Classified Information."

It was prepared by the National Security Council, in accordance with the provisions of Executive Order No. 11030, as amended.

On behalf of the Director of the Office of Management and Budget, I would appreciate receiving any comments you may have concerning this proposal. If you have any comments or objections, they should be received no later than close of business Wednesday, April 12, 1995. Please be advised that agencies that do not respond by the April 12, 1995 deadline will be recorded as not objecting to the proposal.

Comments or inquiries may be submitted by telephone to Mr. Mac Reed of this office (Phone: 395-3563; Fax: 395-7294).

Thank you.

Attachments - Distribution List
Proposed Executive Order

cc: Alice Rivlin
Bob Litan
Gordon Adams
T.J. Glauthier
Joe Minarik
Ken Apfel
Nancy-Ann Min
Sally Katzen
Steve Kelman
Bill Halter

DISTRIBUTION LIST

Honorable Warren Christopher
Secretary
Department of State

Honorable Robert E. Rubin
Secretary
Department of the Treasury

Honorable William Perry
Secretary
Department of Defense

Honorable Richard Rominger
Acting Secretary
Department of Agriculture

Honorable Henry G. Cisneros
Secretary
Department of Housing and Urban Development

Honorable Janet Reno
United States Attorney General

Honorable Ron Brown
Secretary
Department of Commerce

Honorable Federico Pena
Secretary
Department of Transportation

Honorable Bruce Babbitt
Secretary
Department of the Interior

Honorable Robert Reich
Secretary
Department of Labor

Honorable Richard W. Riley
Secretary
Department of Education

Honorable Donna E. Shalala
Secretary
Department of Health and Human Services

Honorable Hazel O'Leary
Secretary
Department of Energy

Honorable Jesse Brown
Secretary
Department of Veterans Affairs

Honorable Carol M. Browner
Administrator
Environmental Protection Agency

Honorable R. James Woolsey
Director
Central Intelligence Agency

Honorable Daniel S. Goldin
Administrator
National Aeronautics and Space Administration

Honorable James B. King
Director
Office of Personnel Management

Honorable Ivan Selin
Chairman
Nuclear Regulatory Commission

Honorable John D. Holum
Director
United States Arms Control and Disarmament Agency

Honorable Carol Rasco
Assistant to the President for
Domestic Policy

Honorable Abner Mikva
Counsel to the President

Honorable John Podesta
Assistant to the President
and Staff Secretary

Honorable Jack Quinn
Chief of Staff to the Vice President

DRAFT
March 29, 1995

Executive Order

Access to Classified Information

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

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

General

Section 1.1 Definitions.

(a) "Agency" has the meaning provided in 44 U.S.C. 3502(1).

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Classified information" means information that has been determined pursuant to Executive Order No. 12356, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that is so designated.

(d) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency; a consultant to an agency; an industrial or commercial contractor of an agency, including all subcontractors; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(e) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(f) "Need for access" means a determination made by an agency head that an employee requires access to a particular level of classified information in order to perform a lawful and authorized function.

(g) "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 a lawful and authorized function.

(h) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(i) "Special Access Program" has the meaning provided in section 4.2 of Executive Order No. 12356, or a successor order.

Sect. 1.2 Access to Classified Information.

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Access to classified information shall be limited to employees who:

(1) are citizens of the United States;

(2) have been determined to be eligible for access under section 3.1(b) of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(3) have a demonstrated need-to-know; and

(4) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of

access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of three years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Sect. 1.3 Financial Disclosure.

(a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who requires access to information that, in the discretion of the agency head, would reveal:

(1) the identity of a covert agent as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of (A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or (B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the

spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sect. 1.4 Use of Automated Financial Record Data Bases.

As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts,

transactions under $10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sect. 1.5 Employee Education and Assistance.

The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to:

(a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

Part 2

Access Eligibility Policy and Procedure

Sect. 2.1 Eligibility Determinations.

(a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability

determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-

time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sect. 2.2 Level of Access Approval.

(a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program may be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs) or intelligence sources and

methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sect. 2.3 Temporary Access to Higher Levels.

(a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where such access:

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 180 days; and

(3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) involves another agency's classified information, that agency must concur before access is granted to its information.

Sect. 2.4 Reciprocal Acceptance of Access Eligibility Determinations.

(a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a Special Access Program shall not be denied eligibility for access to another Special Access Program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a Special Access Program or for candidates for detail or assignment to their agencies, but only where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under section 2.3 or 3.3 of this order or where the determination of

eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sect. 2.5 Specific Access Requirement.

(a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sect. 2.6 Access by Non-United States Citizens.

(a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, or contracts for which access to

classified information is needed. Such individuals shall not be eligible for access to any greater level of classified information than the United States government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only where at least the prior ten years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

Part 3

Access Eligibility Standards

Sect. 3.1 Standards.

(a) No employee shall be deemed to be eligible for access to classified information merely by reason of federal service or contracting, licensee, or grantee status, or as a matter of right

or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in section 3.3 and 2.6 of this order, eligibility for access to classified information shall be granted only to United States citizens as to whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States government does not discriminate on the basis of race, color, religion, sex, national origin, disability,

or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in section 3.1 of this order may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in granting access to classified information. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to

classified information, including access to Special Access Programs.

Sect. 3.2 Basis for Eligibility Approval.

(a) Eligibility determinations for access to classified information shall be based on information concerning the employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and be made part of the employee's security record. Employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its

implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

(d) Nothing in this order shall limit the authority of the Central Intelligence Agency, the National Security Agency, the Department of Defense, the Department of the Treasury, the National Reconnaissance Office, or the Federal Bureau of Investigation to continue to use polygraph interviews of a scope deemed appropriate to their personnel security programs.

Sect. 3.3 Special Circumstances.

(a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway, and the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately

terminated, along with any assignment requiring an access eligibility approval, if such eligibility is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the action.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head exercising statutory authority to waive requirements for granting access to classified information.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years, provided they have remained employed by the same employer during the period in question, the individual certifies in writing that there has been no change in

the relevant information provided in the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior five years and who have been retired or otherwise separated from United States government employment for not more than two years, provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the information provided in the last background investigation, and an appropriate record check is favorable.

Sect. 3.4 Reinvestigation Requirements.

(a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated at any time there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

(d) Whenever any employee becomes aware of information that raises doubts as to whether an employee's continued eligibility for access to classified information is clearly consistent with the national security, such information shall be forwarded to the agency that granted such access.

Part 4 Investigations for Foreign Governments

Sect. 4.1 Authority.

Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the

United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

Part 5 Review of Access Determinations

Sect. 5.1 Determinations of Need for Access.

A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination. This determination shall be conclusive.

Sect. 5.2 Determinations of Eligibility for Access.

(a) Applicants and employees who are determined not to meet the standards established in Part 3 of this order for access to classified information shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit and, upon request and as permitted by the national security and other applicable law, any documents upon which a proposed denial or revocation is based;

(2) informed of their right to be represented by counsel at their own expense;

(3) provided a reasonable opportunity to reply in writing and to request a review of the determination;

(4) provided written notice of the results of the review and the identity of the deciding authority; and

(5) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be final, except as provided in subsection 5.2(b) of this order; and

(6) provided an opportunity to appear personally at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection 5.2(a)(5) based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads, at their sole discretion and as resources and national security considerations permit, may provide additional

review proceedings beyond those required by subsection (a). This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) The procedures set forth in this section shall not be made available where the head of an agency or the principal deputy personally certifies that to do so in a particular case would damage the national security interests of the United States by revealing classified information. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations

of suitability for employment. Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

Part 6 Implementation

Sect. 6.1 Agency Implementing Responsibilities.

Heads of agencies that grant employees access to classified information shall:

(a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include an active oversight and continuing security education and awareness program to ensure effective implementation of this order; and

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines.

(c) conduct periodic evaluations of the agency's implementation and administration of this order. Copies of each report shall be provided to the Security Policy Board.

Sect. 6.2 Employee Responsibilities.

Employees who are granted eligibility for access to classified information occupy positions of high trust and confidence, and shall:

(a) protect classified information in their custody from unauthorized disclosure;

(b) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(c) report all violations of security regulations to the appropriate security official; and

(d) comply with all other security requirements set forth in this order and its implementing regulations.

Sect. 6.3 Sanctions.

Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access

to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulation.

Part 7 General Provisions

Sect. 7.1 Classified Information Procedures Act.

Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. app. 1).

Sect. 7.2 General.

(a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may be disseminated outside the agency only:

(1) to the agency employing the employee who is the subject of the records or information;

(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

(3) to any agency if such information is clearly relevant to the authorized responsibilities of such agency.

(b) The Attorney General, on request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12356 or a successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the Executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the

United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order shall become effective upon publication in the Federal Register.

3-28-95

John,

Attached is the revised text we agreed to on Sec 5.2 of the "Classification" order. Steve Garfinkel requests one additional change (see memo). Let me know which version you approve. Thank you.

Moe

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

March 27, 1995 95 MAR 28 P4:14

MEMORANDUM FOR: Mac Reed
Office of General Counsel

FROM: Steve Garfinkel
Information Security Oversight Office

SUBJECT: Sections 5.2 and 5.3 of proposed Executive order on "Classified National Security Information"

As requested, please find attached revised Sections 5.2 and 5.3 of the subject order. We have amended these sections in accordance with the mark-up that you provided us, following a meeting on these provisions that you attended earlier today.

Please note that we are providing you two versions. The first is strictly in accordance with the mark-up. The second is identical to the first, except that it references a fourth directive to be issued by OMB, i.e., a directive on classification and marking principles. The first version's recitation of pertinent directives leaves a very serious gap in implementation that this reference will correct. ISOO doubts that any of the parties at today's meeting will object to the inclusion of this additional directive, and urges that this second version be adopted.

A directive on classification and marking principles is the most critical for implementation of the order. In addition to prescribing markings, such a directive will explain and implement the classification principles in the order, including standards, challenges, portion marking waivers, agency declassification plans,and the like. Under the current system, these principles are included in ISOO Directive No. 1, which also includes the provisions on safeguarding. Since the safeguarding directive is to be reserved for the Security Policy Board, the remaining components of ISOO Directive No. 1 must be covered in a separate directive.

Please also find attached for your review a revision of those pages of the order that pertain to the Information Security Policy Advisory Council. We have modified this section in accordance with the recommendations of the Federal Advisory Committee Secretariat at the General Services Administration.

Attachments

Section 5.2 *Program Direction.*

(a) The Director of the Office of Management and Budget, in consultation with the Asssistant to the President for National Security Affairs, 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) agency security education and training programs;

(2) agency self-inspection programs; and

(3) 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 issue a directive on safeguarding classified information. This directive shall pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information.

Section 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 and 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 of the 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 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.

Section 5.2 *Program Direction.*

(a) The Director of the Office of Management and Budget, in consultation with the Asssistant to the President for National Security Affairs, 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.

← John, Is this change okay with you?

(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 issue a directive on safeguarding classified information. This directive shall pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information.

Section 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 and 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 of the 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 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.

Section 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 four 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. The President shall appoint the Council chair. 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 policies established under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations, through the Assistant to the President for National Security Affairs, to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) 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) The staff of the Information Security Oversight Office shall provide operational and administrative support for the Council.

(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.

~~Executive Order~~

~~Classified National Security Information~~

This ~~O~~order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed ~~concerning~~of the activities of their ~~G~~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 ~~G~~government.

NOW, 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:

~~As used in this Order, these terms are defined as follows:~~

(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 ~~O~~order or any predecessor order to require protection against unauthorized disclosure.

(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" has the meaning provided at 5 U.S.C. ~~§ 552(f)~~105.

(j) "Senior agency official" means the official designated by the agency head under ~~S~~section 5.6(a)(3) of this ~~O~~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.

Section 1.2 *Classification Standards.*

(a) Information may be originally classified under the terms of this ~~O~~order only if all of the following conditions are met:

(1) ~~A~~an original classification authority is classifying~~ies~~ 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 ~~S~~section 1.5 of this ~~O~~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~~er~~ 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) ~~A~~amplify or modify the substantive criteria or procedures for classification; or~~and~~

(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.

Section 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.

Section 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 pursuant 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 ~~O~~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 ~~O~~order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this ~~O~~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 ~~O~~order and its implementing directives. The information shall be transmitted promptly as provided under this ~~O~~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 thirty (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.

Section 1.5 *Classification Categories.*

Information may not be considered for classification unless it concerns:

(a) ~~M~~military plans, weapons systems, or operations;

(b) ~~F~~foreign government information;

(c) ~~I~~intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) ~~F~~foreign relations or foreign activities of the United States, including confidential sources;

(e) ~~S~~scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) ~~V~~vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Section 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 ~~automatic~~ declassification ten 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 ~~a~~successive periods not to exceed ten ~~additional~~ years at a time if such action is consistent with the standards and procedures established under this ~~O~~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 ~~automatic~~ declassification within ten 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) ~~R~~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, ~~or~~ 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 ~~O~~order.

Section 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) ~~O~~one of the three classification levels defined in ~~S~~section 1.3 of this ~~O~~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 ~~S~~section 1.6(a) or ~~S~~section 1.6(c); or

(B) the date that is ten years from the date of original classification, as prescribed in ~~S~~section 1.6(b); or

(C) the exemption category from automatic declassification, as prescribed in ~~S~~section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in ~~S~~section 1.5 of this ~~O~~order.

(b) Specific information contained in paragraph (a), above, ~~shall~~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 automatic declassification under ~~S~~section 1.6(d) of this ~~O~~order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this ~~O~~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 ~~designations~~ implementing the provisions of this ~~O~~order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued by the Director of the Information Security Oversight Office.

(e) Foreign government information shall retain its original classification markings or shall be assigned a United States 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, ~~H~~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.

Section 1.8 *Classification Prohibitions and Limitations.*

(a) In no case shall information be classified in order to:

(1) ~~C~~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 ~~S~~section 3.6 of this ~~O~~order only if such classification meets the requirements of this ~~O~~order and is accomplished on a document-by-document basis under the personal participation or direction of the agency head, the deputy agency head, or the senior agency official designated under ~~S~~section 5.6 of this ~~O~~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) ~~M~~meets the standards for classification under this ~~O~~order; and

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

As used in this ~~O~~order, "compilation" means an ~~arrangement~~aggregation of pre-existing unclassified items of information ~~gathered together~~.

Section 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 by the Director of the Information Security Oversight Office, an agency head or senior agency official shall establish procedures under which authorized holders of information ~~shall~~ 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 ~~S~~section 5.4 of this ~~O~~order.

Part 2

Derivative Classification

Section 2.1 *Definitions.* For purposes of this order:

~~As used in this Order, these terms are defined as follows:~~

(a) "Derivative classification" means the ~~act of~~ 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 ~~which~~ 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.

Section 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) ~~O~~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.

Section 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 ~~O~~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 ~~O~~order.

Part 3

Declassification and Downgrading

Section 3.1 *Definitions.* For purposes of this order:

~~As used in this Order, these terms are defined as follows:~~

(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 ~~O~~order.

(c) "Declassification authority" means:

(1) ~~T~~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 ~~S~~section 3.6 of this ~~O~~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.

Section 3.2 *Authority for Declassification.*

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this ~~O~~order.

(b) It is presumed that information that continues to meet the classification requirements under this ~~O~~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 ~~a~~the senior agency official ~~with responsibility for processing Freedom of Information Act requests or mandatory review requests under this Order~~. 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) ~~A~~amplify or modify the substantive criteria or procedures for classification; ~~and~~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 ~~O~~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 ~~National Security Council~~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 ~~S~~section shall also apply to agencies that, under the terms of this ~~O~~order, do not have original classification authority, but had such authority under predecessor orders.

Section 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 ~~O~~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 ~~O~~order. Such information may be declassified or downgraded by the agency in possession 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 of the United States as of the effective date of this ~~O~~order shall be declassified or downgraded by the Archivist of the United States in accordance with this ~~O~~order, the directives of the Information Security Oversight Office, ~~and~~ agency declassification guides, and any existing procedural agreement between the Archivist of the United States 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 of the

United States ("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 ~~S~~sections 1.6 and 3.4 of this ~~O~~order.

Section 3.4 *Automatic Declassification.*

(a) Subject to paragraph (b), below, within five years from the issuance of this ~~O~~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) ~~R~~reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair United States cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a United States weapon system;

(5) reveal actual United States 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; ~~or~~

(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

(~~7~~9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this ~~O~~order, an agency head shall notify the President through the Assistant to the President for National Security Affairs~~National Security Council~~ 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~~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, 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 it becomes ~~subject to automatic declassification~~ automatically declassified under this ~~S~~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~~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, 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~~National Security Council~~. The information will remain classified while such an appeal is pending.

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

(f) Information exempted from automatic declassification under this ~~S~~section shall remain subject to the mandatory and systematic declassification review provisions of this ~~O~~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 ~~S~~section for a period longer than 25 years from the date of their creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this ~~S~~section.

Section 3.5 *Systematic Declassification Review.*

(a) Each agency that has originated classified information under this ~~O~~order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records excepted from automatic declassification under ~~S~~section 3.4 of this ~~O~~order. Agencies shall prioritize the systematic review of records based upon:

(1) ~~R~~recommendations of the Information Security Policy Advisory Council, established in ~~S~~section 5.5 of this ~~O~~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 United States shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives ~~of the United States~~ as of the effective date of this

~~O~~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~~prioritize~~ 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 ~~O~~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.

Section 3.6 *Mandatory Declassification Review.*

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

(1) ~~T~~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 two years. If the agency has reviewed the information within the past two 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) ~~others specifically providing advice and counsel to the incumbent President or acting on behalf of the incumbent President~~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 ~~O~~order. They shall release this information unless withholding is otherwise authorized and necessary under applicable law.

(d) In accordance with directives issued pursuant to this ~~O~~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 ~~also~~ 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, ~~and~~ 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 ~~T~~the Archivist shall develop special procedures for the review of information accessioned into the National Archives ~~of the United States~~.

Section 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 ~~O~~order, or pursuant to the automatic declassification or systematic review provisions of this ~~O~~order:

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

Section 3.8 *Declassification Database.*

(a) The Archivist of the United States, in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information 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 provided by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

Part 4

Safeguarding

Section 4.1 *Definitions.* For purposes of this order:

~~As used in this Order, these terms are defined as follows:~~

(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 a lawful and authorized 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 ~~which~~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.

Section 4.2 *General Restrictions on Access.*

(a) A person may have access to classified information provided that:

(1) ~~A~~a favorable determination of ~~trustworthiness~~ 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 Aauthorized to disseminateion of 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, whichthat collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) Pprevent 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 Oorder, 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 ~~by the President through the National Security Council~~pursuant to this order, classified information originating in one agency may not be disseminated outside 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 ~~S~~section, the Department of Defense shall be considered one agency.

Section 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.

Section 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) ~~T~~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 ~~extra~~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 promulgated by the Director of the Information Security Oversight Office.

(3) Special access programs shall be subject to the oversight program established under ~~S~~section 5.6(a)(3) of this ~~O~~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 ~~O~~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 ~~and the Executive Secretary of the National Security Council or designee~~ shall review annually each special access program to determine whether it continues to meet the requirements of this ~~O~~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 ~~O~~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 ~~O~~order. Each existing special access program that an agency head or principal deputy ~~re~~validates shall be treated as if it were established on the effective date of this ~~O~~order.

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

Section 4.5 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in ~~S~~section 4.2(a)(3) of this ~~O~~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) ~~A~~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 ~~S~~section may be granted only if the agency head or senior agency official of the originating agency:

(1) ~~D~~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 ~~O~~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

Section 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 ~~O~~order and its implementing directives.

(b) "Violation" means:

(1) ~~A~~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 ~~O~~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 ~~O~~order.

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

Section 5.2 *Policy Direction.*

(a) The President, through the Assistant to the President for National Security Affairs,~~National Security Council~~ shall provide overall policy guidance for the program established under this ~~O~~order.

(b) The Director of the Information Security Oversight Office shall be responsible for implementing and monitoring the program established under this ~~O~~order.

Section 5.3 *Information Security Oversight Office.*

(a) There is established an Information Security Oversight Office.

(1) Remainder Reserved.

(b) The Director shall:

(1) ~~D~~develop, in consultation with the agencies, and promulgate, subject to the ~~approval~~concurrence of the Assistant to the President for

National Security Affairs~~National Security Council~~, directives for the implementation of this ~~O~~order, which shall be binding on the agencies;

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

(3) review agency implementing regulations and agency guides for systematic declassification review. The Director shall require any regulation or guide to be changed if inconsistent with this ~~O~~order or its implementing directives. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs~~National Security Council~~. The agency regulation or guide shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of each agency's program established under this ~~O~~order, and to require of each agency, those reports, information, and other cooperation that may be necessary to fulfill the Director's 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 President through the Assistant to the President for National Security Affairs~~National Security Council~~ within 60 days of the Director's request for access. Access shall be denied pending a prompt decision ~~by the National Security Council~~;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;

(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 ~~O~~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 ~~O~~order;

(8) report at least annually to the President through the Assistant to the President for National Security Affairs~~National Security Council~~ on the implementation of this ~~O~~order; and

(9) have the authority to convene and chair interagency or other meetings to discuss matters pertaining to the program established under this ~~O~~order.

(c) Directives issued by the Director of the Information Security Oversight Office shall establish uniform standards for:

(1) ~~S~~safeguarding classified information;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

Section 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 ~~Executive Secretary of the National Security Council~~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 designate the Chairman 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 Chairman. The Chairman 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) ~~D~~decide on appeals by persons who have filed classification challenges under ~~S~~section 1.9 of this ~~O~~order;

(2) approve, deny or amend agency exemptions from automatic declassification as provided in ~~S~~section 3.4 of this ~~O~~order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under ~~S~~section 3.6 of this ~~O~~order.

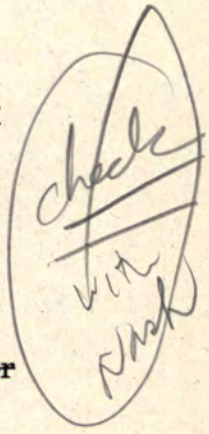
(c) *Rules and Procedures.* The Panel shall issue by-laws, which shall be published in the *Federal Register* no later than 120 days from the effective date of this ~~O~~order. The by-laws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that: ~~(1) T~~the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; ~~and~~ (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 two years.

~~(2) the Panel will assure compliance with the safeguarding requirements established by this Order and its implementing directives; and~~

(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~~National Security Council~~. ~~(3)~~ ~~t~~The Panel will report to the President through the Assistant to the President for National Security Affairs~~National Security Council~~ any instance in which it believes that an agency head is not cooperating fully with the Panel.

Section 5.5 *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be comprised of seven members appointed by the President for staggered terms not to exceed four years, from among ~~interested~~ 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. The members shall elect the Council ~~C~~chair~~man~~. ~~The Council's by-laws shall establish standards for length of member service and rotation of the chair.~~



(b) *Functions.* The Council shall:

(1) ~~A~~advise the President, the Assistant to the President for National Security Affairs~~National Security Adviser~~, the Director of the Information Security Oversight Office, or such other executive branch officials as it deems appropriate, on policies established under this ~~O~~order or its implementing directives, including recommended changes to those policies;

(2) recommend to agency heads specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) The Council shall meet at least twice each calendar year, and as otherwise provided in its by-laws.

(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) The staff of the Information Security Oversight Office shall provide operational and administrative support for the Council.

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

Section 5.6 *General Responsibilities.*

(a) Heads of agencies that originate or handle classified information shall:

(1) ~~D~~demonstrate personal commitment and commit senior management to the successful implementation of the program established under this ~~O~~order;

(2) commit necessary resources to the effective implementation of the program established under this ~~O~~order;

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

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

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

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

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

(E) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified 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;

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

(G) 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) ~~O~~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; ~~and~~

(H) accounting for the costs associated with the implementation of this ~~O~~order, which shall be reported to the Director of the Information Security Oversight Office for publication~~.~~; and

(I) 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 which no longer exists and for which there is no clear successor in function.

(b) The Inspector General of each agency shall conduct periodic evaluations of the agency's implementation and administration of the program established under this ~~O~~order. To the extent permitted by statute, those portions of each Inspector General's reports that deal with this program shall be provided to the agency head and the Director of the Information Security Oversight Office.

Section 5.7 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this ~~O~~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) ~~D~~disclose to unauthorized persons information properly classified under this ~~O~~order or predecessor orders;

(2) classify or continue the classification of information in violation of this ~~O~~order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this ~~O~~order; or

(4) contravene any other provision of this ~~O~~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 ~~O~~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

Section 6.1 *General Provisions.*

(a) Nothing in this ~~O~~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 ~~O~~order with respect to any question arising in the course of its administration.

(c) Nothing in this ~~O~~order~~rder~~ 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.

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

Section 6.2 *Effective Date.*

This ~~O~~order shall become effective 180 days from the date of its issuance.