Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

federal register

Tuesday
April 6, 1982

Part IV

The President

Executive Order 12356—
National Security Information

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Federal Register
Vol. 47, No. 66
Tuesday, April 6, 1982

Presidential Documents

Title 3—

The President

Executive Order 12356 of April 2, 1982

National Security Information

TABLE OF CONTENTS

[FR Page]

Preamble ..... [14874]

Part 1. Original Classification

1.1 Classification Levels ..... [14874]
1.2 Classification Authority ..... [14874]
1.3 Classification Categories ..... [14875]
1.4 Duration of Classification ..... [14876]
1.5 Identification and Markings ..... [14877]
1.6 Limitations on Classification ..... [14877]

Part 2. Derivative Classification

2.1 Use of Derivative Classification ..... [14878]
2.2 Classification Guides ..... [14878]

Part 3. Declassification and Downgrading

3.1 Declassification Authority ..... [14878]
3.2 Transferred Information ..... [14879]
3.3 Systematic Review for Declassification ..... [14879]
3.4 Mandatory Review for Declassification ..... [14879]

Part 4. Safeguarding

4.1 General Restrictions on Access ..... [14880]
4.2 Special Access Programs ..... [14881]
4.3 Access by Historical Researchers and Former Presidential Appointees ..... [14881]

Part 5. Implementation and Review

5.1 Policy Direction ..... [14881]
5.2 Information Security Oversight Office ..... [14881]
5.3 General Responsibilities ..... [14882]
5.4 Sanctions ..... [14882]

Part 6. General Provisions

6.1 Definitions ..... [14883]
6.2 General ..... [14883]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

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

Part 1

Original Classification

Section 1.1 *Classification Levels.*

(a) National security information (hereinafter "classified information") shall 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.

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

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

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 *Classification Authority.*

(a) *Top Secret.* The authority to classify information originally as Top Secret may be exercised only by:

(1) the President;

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

(3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret.* The authority to classify information originally as Secret may be exercised only by:

(1) agency heads and officials designated by the President in the **Federal Register**;

(2) officials with original Top Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential.* The authority to classify information originally as Confidential may be exercised only by:

(1) agency heads and officials designated by the President in the **Federal Register**;

(2) officials with original Top Secret or Secret classification authority; and

(3) officials delegated such authority pursuant to Section 1.2(d).

(d) *Delegation of Original Classification Authority.*

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

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification author-

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

ity; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 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.

Sec. 1.3 *Classification Categories.*

(a) Information shall be considered for classification if it concerns:

(1) military plans, weapons, or operations;

(2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) foreign government information;

(4) intelligence activities (including special activities), or intelligence sources or methods;

(5) foreign relations or foreign activities of the United States;

(6) scientific, technological, or economic matters relating to the national security;

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

(8) cryptology;

(9) a confidential source; or

(10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Sec. 1.4 *Duration of Classification.*

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 *Identification and Markings.*

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

(1) one of the three classification levels defined in Section 1.1;

(2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;

(3) the agency and office of origin; and

(4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 *Limitations on Classification.*

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to 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) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information 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 this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 *Use of Derivative Classification.*

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(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 designated under Section 5.3(a)(1); and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 *Declassification Authority.*

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

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

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

Sec. 3.2 *Transferred Information.*

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

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in 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 shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 *Systematic Review for Declassification.*

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(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.

Sec. 3.4. *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 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. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) 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 shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) 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, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 *General Restrictions on Access.*

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, 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. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 *Special Access Programs.*

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. 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.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

Sec. 4.3 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

(1) are engaged in historical research projects, or

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

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

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

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

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

Part 5

Implementation and Review

Sec. 5.1 *Policy Direction.*

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 *Information Security Oversight Office.*

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

(b) The Director shall:

(1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;

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

(3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;

(4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;

(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 information security program;

(7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;

(8) report at least annually to the President through the National Security Council on the implementation of this Order; and

(9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 *General Responsibilities.*

Agencies that originate or handle classified information shall:

(a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;

(b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the **Federal Register** to the extent that these regulations affect members of the public;

(c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable 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; and

(d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.

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

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(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) Each agency head or the senior official designated under Section 5.3(a)(1) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 *Definitions.*

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or 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.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

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

(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.

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

(f) "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, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 *General.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order,

(e) This Order shall become effective on August 1, 1982.

Ronald Reagan

THE WHITE HOUSE,
April 2, 1982.

[FR Doc. 82-9320
Filed 4-2-82; 2:52 pm]
Billing code 3195-01-M

Editorial Note: The President's statement of Apr. 2, 1982, on signing Executive Order 12356 is printed in the *Weekly Compilation of Presidential Documents* (vol. 18, no. 13)

Approved For Release 2005/12/01 : CIA-RDP93B01194R001200040001-4

INFORMATION SECURITY OVERSIGHT OFFICE

32 CFR Part 2001

National Security Information

AGENCY: Information Security Oversight Office (ISOO).

ACTION: Final rule.

SUMMARY: The information Security Oversight Office is publishing this amendment to its Directive No. 1, implementing Executive Order 12356 (47 FR 14874, April 6, 1982), pursuant to section 5.2(b)(1) of the Executive Order. The National Security Council approved the issuance of this amendment on May 8, 1984. This amendment to § 2001.47 provides instructions to agencies on the preparation of damage assessments following the loss or possible compromise of national security information.

EXECUTIVE DATE: May 16, 1984.

FOR FURTHER INFORMATION CONTACT: Steven Garfinkel, Director, ISOO (202) 535-7251.

SUPPLEMENTARY INFORMATION: This amendment to ISOO Directive No. 1 is issued pursuant to section 5.2(b)(1) of Executive Order 12356.

List of Subjects in 32 CFR Part 2001

Classified information.

PART 2001—[AMENDED]

32 CFR Part 2001 is amended by revising § 2001.47 to read as follows:

§ 2001.47 Loss or Possible Compromise [4.1(b)].

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to an official designated for this purpose by the person's agency or organization. The agency that originated the information shall be notified of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise. The following guidelines shall govern the conduct of damage assessments:

(a) *Initiation of Damage Assessments.* An agency head shall initiate a damage assessment whenever there has been a compromise of classified information originated by that agency that, in his or her judgment, can reasonably be expected to cause damage to the national security. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, unauthorized sales, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date, and circumstances of the compromise.

(2) Classification of the specific information lost.

(3) A description of the specific information lost.

(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

(6) An assessment of whether (i) the classification of the information involved should be continued without change; (ii) the specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; (iii) downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change.

(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(8) An assessment of other appropriate corrective, administrative, disciplinary or legal actions.

(c) *System of Control of Damage Assessments.* Each agency shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in paragraph (a), and that records are maintained in a manner that facilitates their retrieval and use within the agency.

(d) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, each department or agency undertaking a damage assessment shall advise other agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment.

(2) Whenever a compromise occurs within an agency that is not responsible for the damage assessment, that agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(3) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the agency performing the damage assessment shall ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with appropriate agency legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment shall coordinate with the Department of Justice.

(5) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI) has occurred.

(Sec. 5.2(b)(1), E.O. 12356)

Dated: May 11, 1984.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 84-13148 Filed 5-15-84; 8:45 am]

BILLING CODE 6820-AF-M