AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FBI investigate domestic threats in this time of war, additional funding for the Coast Guard for port security in the United States and in the Middle East.

In this time of heightened security, we are expecting States and communities to take on greater responsibilities to protect critical infrastructure. And so I'm seeking additional resources to help States and cities make these preparations for the protection of our citizens.

Yesterday I informed the leaders of Congress of these spending requests. The situation in any war is fluid. I reminded them of that fact, and so I'm asking Congress for flexibility in how these funds can be allocated. They heard that message. They also heard the message that the need is urgent. The wartime supplemental is directly related to winning this war and to securing the peace that will follow this war. I ask Congress to act quickly and responsibly.

One thing is for certain: Business as usual on Capitol Hill can't go on during this time of war. And by that I mean the supplemental should not be viewed as an opportunity to add spending that is unrelated, unwise, and unnecessary. Every dollar we spend must serve the interest of our Nation, and the interest of our Nation in this supplemental is to win this war and to be able to keep the peace.

Eighteen months ago, this building came under attack. From that day to this, we have been engaged in a new kind of war, and we are winning. We will not leave our future to be decided by terrorist groups or terrorist regimes. At every turn in this conflict, Americans can be confident in the people who wear our Nation's uniform. We support them. We are thankful for their service in places of great danger, in this hour of great need.

May God continue to look out after those who defend the peace and freedom. And may God continue to bless America. Thank you.

NOTE: The President spoke at 10:30 a.m. in the Eisenhower Dining Room. In his remarks, he referred to President Saddam Hussein of Iraq; and Gen. Tommy R. Franks, USA, combatant commander, U.S. Central Command. The Office of the Press Secretary also released a Spanish language transcript of these remarks.

Executive Order 13292—Further Amendment to Executive Order 12958, as Amended, Classified National Security Information

March 25, 2003

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further amend Executive Order 12958, as amended, it is hereby ordered that Executive Order 12958 is amended to read as follows:

"Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.

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

Part 1—Original Classification

Sec. 1.1. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably

could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. *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.

Sec. 1.3. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President and, in the performance of executive duties, the Vice President;

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

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

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

(c) Delegation of original classification authority.

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

(2) "Top Secret" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

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

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority

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

Sec. 1.4. *Classification Categories.* Information shall not be considered for classification unless it concerns:

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

(b) foreign government information;

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

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

(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

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

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(h) weapons of mass destruction.

Sec. 1.5. *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. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a) or section 1.5(c);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b); or

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5 (b); and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

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

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

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

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

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

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

(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

(1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;

(2) the information may be reasonably recovered; and

(3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.8. *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) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure 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 (Panel) established by section 5.3 of this order.

Part 2—Derivative Classification

Sec. 2.1. *Use of Derivative Classification.* (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

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

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

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

Sec. 2.2. *Classification Guides.* (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

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

(1) has program or supervisory responsibility over the information or is the senior agency official; and

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

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

Part 3—Declassification and Downgrading

Sec. 3.1. *Authority for Declassification.* (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

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

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

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

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

Sec. 3.2. *Transferred Records.* (a) In the case of classified records 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 records that are not officially transferred as described in paragraph (a) of this section, 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 records shall be deemed to be the originating agency for purposes of this order. Such records 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 records.

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

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone 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 section 3.3 of this order.

Sec. 3.3. *Automatic Declassification.* (a) Subject to paragraphs (b)–(e) of this section, on December 31, 2006, all classified 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 records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as provided in paragraphs (b)–(e) of this section.

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

(1) reveal the identity of a confidential human source, or a human intelligence 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 U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

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

(c) An agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, 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. File series exemptions previously approved by the President shall remain valid without any additional agency action.

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

(1) a description of the information, either by reference to information in specific records or in the form of a declassification guide;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency

head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.

(4) By notification to the Director of the Information Security Oversight Office, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

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

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

(h) Records containing information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies shall be referred for review to those agencies and the information of concern shall be subject to automatic declassification only by those agencies, consistent with the provisions of subparagraphs (e)(3) and (e)(4) of this section.

Sec. 3.4. *Systematic Declassification Review.* (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.

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

Sec. 3.5. *Mandatory Declassification Review.* (a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403–5c, 403–5e, and 431); and

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

(b) Information originated by:

(1) the incumbent President or, in the performance of executive duties, the incumbent Vice President;

(2) the incumbent President's White House Staff or, in the performance of executive duties, the incumbent Vice President's Staff;

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

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records 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 Panel. The information shall remain classified pending a prompt decision on the appeal.

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

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

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

Sec. 3.6. *Processing Requests and Reviews.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

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

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

Sec. 3.7. *Declassification Database.* (a) The Director of the Information Security Oversight Office, in conjunction with those agencies that originate classified information, shall coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(b) Agency heads shall fully cooperate with the Director of the Information Security Oversight Office in these efforts.

Part 4—Safeguarding

Sec. 4.1. *General Restrictions on Access.* (a) A person may have access to classified information provided that:

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

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

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

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) 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.

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

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

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

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(g) 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.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including modified handling and transmission and 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.

(i) Except as otherwise provided by statute, this order, directives implementing this

order, or by direction of the President, classified information originating in one agency shall 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 section, the Department of Defense shall be considered one agency. Prior consent is not required when referring records for declassification review that contain information originating in several agencies.

Sec. 4.2. *Distribution Controls.* (a) Each agency shall establish controls over the distribution of classified information to ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing this order and any procedures issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of Central Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

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

Sec. 4.3. *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 shall 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 when the program is required by statute or upon a specific finding that:

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

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

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

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

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office, or, for special access programs

that are extraordinarily sensitive and vulnerable, to the Director only.

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

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

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

Sec. 4.4. *Access by Historical Researchers and Certain Former Government Personnel.* (a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied policy-making positions to which they were appointed by the President under section 105(a)(2)(A) of title 3, United States Code, or the Vice President under 106(a)(1)(A) of title 3, United States Code; or

(3) served as President or Vice President.

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

(1) determines in writing that access is consistent with the interest of the 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 and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee or a Vice Presidential appointee.

Part 5—Implementation and Review

Sec. 5.1. *Program Direction.* (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant 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 Information Security Oversight Office shall establish standards for:

(1) classification and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

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

Sec. 5.2. *Information Security Oversight Office.* (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

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

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

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

(3) review and approve agency implementing regulations and agency guides for systematic declassification

review prior to their issuance by the agency;

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

(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 Assistant to the President for National Security Affairs;

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

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

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

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

Sec. 5.3. *Interagency Security Classification Appeals Panel.*

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

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

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

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

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

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the *Federal Register*. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;
(2) there is no current action pending on the issue within the Federal courts; and
(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

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

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

(f) Notwithstanding paragraphs (a) through (e) of this section, whenever the Panel reaches a conclusion that information owned or controlled by the Director of Central Intelligence (Director) should be declassified, and the Director notifies the Panel that he objects to its conclusion because he has determined that the information could reasonably be expected to cause damage to the national security and to reveal (1) the identity of a human intelligence source, or (2) information about the application of an intelligence source or method (including any information that concerns, or is provided as a result of, a relationship with a cooperating intelligence element of a foreign government), the information shall remain classified unless the Director's determination is appealed to the President, and the President reverses the determination.

Sec. 5.4. *General Responsibilities.* Heads of agencies that originate or handle classified information shall:

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

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

(c) ensure that agency records systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

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

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
(2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;
(3) establishing and maintaining security education and training programs;
(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;
(5) establishing procedures to prevent unnecessary access to classified information, including procedures that:
(A) require that a need for access to classified information is established before initiating administrative clearance procedures; and
(B) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;
(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
(7) ensuring 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:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information;

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

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

Sec. 5.5. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

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

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

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

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

(4) contravene any other provision of this order or its implementing directives.

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

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

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

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

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

Part 6—General Provisions

Sec. 6.1. *Definitions.* For purposes of this order:

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

(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "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.

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

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

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

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

(g) "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.

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

(i) "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.

(j) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(k) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(l) "Declassification authority" means:

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

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

(3) a supervisory official of either; or

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

(m) "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.

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

(o) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(p) "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.

(q) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(r) "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 Government 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.

(s) "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.

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

(u) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

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

(w) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

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

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

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

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

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

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

(dd) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ee) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(ff) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(gg) "Safeguarding" means measures and controls that are prescribed to protect classified information.

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

(ii) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

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

(kk) "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.

(ll) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to

have permanent historical value in accordance with title 44, United States Code.

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

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

(oo) "Violation" means:

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

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

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

(pp) "Weapons of mass destruction" means chemical, biological, radiological, and nuclear weapons.

Sec. 6.2. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

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

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, officers, employees, or agents. The foregoing is in addition to the specific provisos set forth in sections 3.1(b) and 5.3(e) of this order."

(d) Executive Order 12356 of April 6, 1982, was revoked as of October 14, 1995.

Sec. 6.3. *Effective Date.* This order is effective immediately, except for section 1.6, which shall become effective 180 days from the date of this order.

George W. Bush

The White House,
March 25, 2003.

[Filed with the Office of the Federal Register, 9:17 a.m., March 27, 2003]

NOTE: This Executive order was published in the *Federal Register* on March 28.

Letter to the Speaker of the House of Representatives Transmitting a Supplemental Budget Request To Support Military and Humanitarian Operations in Iraq and To Ensure Domestic Safety

March 25, 2003

Dear Mr. Speaker:

On October 16, 2002, I signed into law the "Authorization for Use of Military Force Against Iraq Resolution of 2002" (Public Law 107–243). After condemning Saddam Hussein's continued possession of chemical and biological weapons, obstruction of inspections, and brutal repression of the Iraqi people, the Congress affirmed, "Iraq poses a continuing threat to the national security of the United States and international peace and security of the Persian Gulf region and remains in material and unacceptable breach of its international obligations."

Subsequent to enactment of Public Law 107–243, the United Nations Security Council unanimously agreed to Resolution 1441 offering Iraq one final chance to disarm. After more than a decade of deceit and defiance, the regime, yet again, failed to "fully and unconditionally" comply. Iraq continues to pose a grave danger to global peace and security. The United States and our allies must seek to disarm Iraq and liberate the Iraqi people, and we will prevail.