Proposed Rules

Federal Register
Vol. 61, No. 181
Tuesday, September 17, 1996

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

OFFICE OF MANAGEMENT AND BUDGET

5 CFR Part 1312

RIN 0348–AB34

Classification, Downgrading, Declassification and Safeguarding of National Security Information

AGENCY: Office of Management and Budget, Executive Office of the President.

ACTION: Notice of proposed rule.

SUMMARY: The Office of Management and Budget (OMB) seeks public comment on a proposed rule that would set forth the procedures to be followed by OMB staff regarding the classification, downgrading, declassification and safeguarding of national security information. In addition, this information lists OMB staff who are authorized to originally classify information at the top secret and secret level. These regulations also contain guidance on the procedures to be used by OMB when other government agencies and the public request that classified information in OMB files be reviewed for possible declassification and release. If such information may not be released these procedures also provide guidance on how to appeal such an action.

DATES: Comments must be received no later than November 18, 1996.

ADDRESSES: Comments on the proposed rule should be addressed to: Darrell A. Johnson, Deputy Assistant Director for Administration, Office of Management and Budget, Room 9026, New Executive Office Building, Washington, D.C. 20503. Comments up to three pages in length may be submitted via facsimile to (202) 395–3504. Electronic mail comments may be submitted via Internet to SECREG@A1.EOP.GOV. Please include the full body of electronic mail comments in the text and not as an attachment. Please include the name, title, organization, postal address, and E-mail address in the text of the message.

FOR FURTHER INFORMATION CONTACT: Darrell A. Johnson, Deputy Assistant Director for Administration, Office of Management and Budget, at (202) 395–5715.

SUPPLEMENTARY INFORMATION: OMB is revising its regulations concerning the classification, downgrading, declassification and safeguarding of national security information. This revision is necessary to ensure conformity with guidelines in Executive Order 12958, April 20, 1995 and its implementing directives. The Office of Management and Budget is repealing its existing Part 1312 and replacing it with the new Part 1312.

Regulatory Flexibility Act, Unfunded Mandates Reform Act, and Executive Orders 12866 and 12875

For purposes of the Regulatory Flexibility Act (5 U.S.C. § 601 et seq.), the proposed rule will not, if promulgated, have a significant economic effect on a substantial number of small entities; the proposed rule addresses only the procedures to be followed in the production or disclosure of OMB materials and information in litigation. For purposes of the Unfunded Mandates Reform Act of 1995 (P.L. 104–4), as well as Executive Orders No. 12866 and 12875, the proposed rule would not significantly or uniquely affect small governments, and would not result in increased expenditures by State, local, and tribal governments, or by the private sector, of $100 million or more.

Issued in Washington, D.C., September 11, 1996.

Jacob J. Lew,

Acting Director.

For the reasons set forth in the preamble, OMB proposes to amend 5 CFR Chapter III by revising Part 1312 to read as follows:

PART 1312—CLASSIFICATION, DOWNGRADING, DECLASSIFICATION AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION

Subpart A—Classification and Declassification of National Security Information

Subpart B—Control and Accountability of Classified Information

Subpart C—Mandatory Declassification Review

Authority: Executive Order 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333.

Subpart A—Classification and Declassification of National Security Information

§ 1312.1 Purpose and authority.

This subpart sets forth the procedures for the classification and declassification of national security information in the possession of the Office of Management and Budget. It is issued under the authority of Executive Order 12958, April 20, 1995, Information Security Oversight Office Directive No 1, (60 FR 53492, October 13, 1995), and is applicable to all OMB employees.

§ 1312.2 Responsibilities.

The effectiveness of the classification and declassification program in OMB depends entirely on the amount of attention paid to it by supervisors and their staffs in those offices and divisions that possess or produce classified material. Officials who originate classified information are responsible

for proper assignment of a classification to that material and for the decision as to its declassification. Officials who produce documents containing classified information must determine the source of the classification for that information and must ensure that the proper identity of that source is shown on the document. Custodians of classified material are responsible for its safekeeping and for ensuring that such material is adequately marked as to current classification. Custodians are also responsible for the control of and accounting for all classified material within their area of jurisdiction as prescribed in OMB Manual Section 1030.

(a) EOP Security Officer. In cooperation with the Associate Director for Administration, the EOP Security Officer supervises the administration of this section and develops programs to assist in the compliance with the Order. Specifically, he:

(1) Promotes the correct understanding of this section by all employees by providing annual security refresher briefings and ensures that new employees attend initial briefings about overall security procedures and policies.

(2) Issues and keeps current such classification guides and guidelines for review for declassification as are required by the Order.

(3) Conducts periodic reviews of classified documents produced and provides assistance and guidance where necessary.

(4) Maintains and publishes a current listing of all officials who have been designated in writing to have Top Secret, Secret, and Confidential original classification authority.

(b) Heads of divisions or offices. The head of each division or major organizational unit is responsible for the administration of this section within his or her area. Appropriate internal guidance should be issued to cover special or unusual conditions within an office.

§ 1312.3 Classification requirements.

United States citizens must be kept informed about the activities of their Government. However, in the interest of national security, certain official information must be subject to constraints on its dissemination or release. This information is classified in order to provide that protection.

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

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

(2) foreign government information;

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

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

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

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

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

(b) When information is determined to meet one or more of the criteria in paragraph (a) of this section, it shall be classified by an original classification authority when he/she determines that its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security.

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

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

§ 1312.4 Classified designations.

(a) Except as provided by the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended, the Executive Order 12958 provides the only basis for classifying information. Information which meets the test for classification may be classified in one of the following three designations:

(1) Top Secret. This classification shall be applied only 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. This classification shall be applied only 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. This classification shall be applied only 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) If there is significant doubt about the need to classify information it shall not be classified. If there is significant doubt about the appropriate level of classification it shall be classified at the lower level.

§ 1312.5 Authority to classify.

(a) The authority to originally classify information or material under these regulations shall be limited to those officials concerned with matters of national security. The officials listed below are granted authority by the Director, OMB, to assign original classifications as indicated to information or material that is originated by OMB staff and relating to the national security of the United States:

(1) Top Secret and below:

(i) Deputy Director.

(ii) Deputy Director for Management.

(iii) Associate Director for National Security and International Affairs.

(iv) Associate Director for Natural Resources, Energy and Science.

(2) Secret and below:

(i) Deputy Associate Director for National Security.

(ii) Deputy Associate Director for International Affairs.

(iii) Deputy Associate Director for Energy and Science.

(b) Classification authority is not delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or from a classification guide.

§ 1312.6 Duration of classification.

(a) When determining the duration of classification for information originally classified under Executive Order 12958, an original classification authority shall follow the following sequence:

(1) He/She shall attempt to determine a date or event that is less than 10 years from the date of original classification, and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction;

(2) If unable to determine a date or event of less than 10 years, he/she shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision;

(3) He/She may extend the duration of classification or reclassify specific information for a period not to exceed 10 additional years if such action is consistent with the exemptions as outlined in Section 1.6(d) of the Executive Order. This provision does

not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under Title 44 United States Code.

(4) May exempt from declassification within 10 years specific information, which is consistent with the exemptions as outlined in Section 1.6 (d) of the Executive Order.

Extending Duration of Classification. Extensions of classification is not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event. If an original classification authority has assigned a date or event for declassification that is 10 years or less from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for additional periods not to exceed 10 years at a time. Records determined to be of historical value may not exceed the duration of 25 years.

(b) When extending the duration of classification, the original classification authority must:

(1) Be an original classification authority with jurisdiction over the information.

(2) Ensure that the information continues to meet the standards for classification under the Executive Order.

(3) Make reasonable attempts to notify all known holders of the information. Information classified under prior orders marked with a specific date or event for declassification is automatically declassified upon that date or event. Information classified under prior orders marked with Originating Agency's Determination Required (OADR) shall:

(i) Be declassified by a declassification authority as defined in Section 3.1 of the Order.

(ii) Be re-marked by an authorized original classification authority with jurisdiction over the information to establish a duration of classification consistent with the Order.

(iii) Be subject to Section 3.4 of the Order if the records are determined to be of historical value and are to remain classified for 25 years from the date of its original classification.

§ 1312.7 Derivative classification.

A ''derivative classification'' means that the information is in substance the same information that is currently classified, usually by another agency or classification authority. The application of derivative classification markings is the responsibility of the person who incorporates, restates, paraphrases, or generates in new form information that is already classified, or one who applies such classification markings in accordance with instructions from an authorized classifier or classification guide. Extreme care must be taken to continue classification and declassification markings when such information is incorporated into OMB documents. The duplication or reproduction of existing classified information is not derivative classification. Persons who use derivative classification need not possess original classification authority.

§ 1312.8 Standard identification and markings.

(a) Original Classification. At the time classified material is produced, the classifier shall apply the following markings on the face of each originally classified document, including electronic media:

(1) Classification Authority. The name/personal identifier, and position title of the original classifier shall appear on the ''Classified By'' line.

(2) Agency and Office of Origin. If not otherwise evident, the agency and office of origin shall be identified and placed below the name on the ''Classified By'' line.

(3) Reasons for Classification. Identify the reason(s) to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in Section 1.5 of the Order.

(4) Declassification instructions. These instructions shall indicate the following:

(i) The duration of the original classification decision shall be placed on the ''Declassify On'' line.

(ii) The date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which may not exceed 10 years from the date of the original decision.

(iii) When a specific date or event within 10 years cannot be established, the classifier will apply the date that is 10 years from the date of the original decision.

(iv) The exemption category from declassification. Upon determination that the information must remain classified beyond 10 years, the classifier will apply the letter ''X'' plus a brief recitation of the exemption category(ies), or the letter ''X'' plus the number that corresponds to the exemption category(ies) in Section 1.6(d) of the Order.

(v) An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. The ''Declassify On'' line shall be revised to include the new declassification instructions and shall include the identity of the person authorizing the extension and the date of the action.

(vi) Information exempted from automatic declassification at 25 years should on the ''Declassify On'' line be revised to include the symbol ''25X'' plus a brief reference to the pertinent exemption categories/numbers of the Executive Order.

(5) The overall classification of the document is the highest level of information in the document and will be conspicuously placed stamped at the top and bottom of the outside front and back cover, on the title page, and on the first page.

(6) The highest classification of individual pages will be stamped at the top and bottom of each page, to include ''unclassified'' when it is applicable.

(7) The classification of individual portions of the document, (ordinarily a paragraph, but including subjects, titles, graphics) shall be marked by using the abbreviations (TS), (S), (C), or (U), will be typed or marked at the beginning or end of each paragraph or section of the document. If all portions of the document are classified at the same level, this may be indicated by a statement to that effect.

(b) Derivative Classification. Information classified derivatively on the basis of source documents shall carry the following markings on those documents:

(1) The derivative classifier shall concisely identify the source document(s) or the classification guide on the ''Derived From'' line, including the agency and where available the office of origin and the date of the source or guide. When a document is classified derivatively on the basis of more than one source document or classification guide, the ''Derived From'' line shall appear as ''Derived From: Multiple Sources''.

(2) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. Where practicable the copies of the document should also have this list attached.

(3) A document derivatively classified on the basis of a source document that is itself marked ''Multiple Sources''

shall cite the source document on its ''Derived From'' line rather than the term ''Multiple Sources''.

(4) The reason for the original classification decision, as reflected in the source document, is not required to be transferred in a derivative classification action.

(5) Declassification instructions shall carry forward the instructions on the ''Declassify On'' line from the source document to the derivation document or the duration instruction from the classification guide. Where there are multiple sources, the longest duration of any of its sources shall be used.

(6) When a source document or classification guide contains the declassification instruction ''Originating Agency's Determination Required'' (OADR) the derivative document shall carry forward the fact that the source document(s) were so marked and the date of origin of the most recent source document(s).

(7) The derivatively classified document shall be conspicuously marked with the highest level of classification of information.

(8) Each portion of a derivatively classified document shall be marked in accordance with its source.

(9) Each office shall, consistent with Section 3.8 of the order, establish and maintain a database of information that has been declassified.

(c) Additional Requirements. (1) Markings other than ''Top Secret'', ''Secret'', and ''Confidential'' shall not be used to identify classified national security information.

(2) Transmittal documents will be stamped to indicate the highest classification of the information transmitted, and shall indicate conspicuously on its face the following or something similar ''Unclassified When classified Enclosure Removed'' to indicate the classification of the transmittal document standing alone.

(3) The classification data for material other than documents will be affixed by tagging, stamping, recording, or other means to insure that recipients are aware of the requirements for the protection of the material.

(4) Documents containing foreign government information shall include the markings ''This Document Contains (country of origin) Information'' * * * If the identity of the specific government must be concealed, the document shall be marked ''This Document Contains Foreign Government Information,'' and pertinent portions marked ''FGI'' together with the classification level, e.g., ''(FGI–C)''. In such cases, separate document identifying the government shall be maintained in order to facilitate future declassification actions.

(5) Documents, regardless of medium, which are expected to be revised prior to the preparation of a finished product—working papers—shall be dated when created, marked with highest classification, protected at that level, and destroyed when no longer needed. When any of the following conditions exist, the working papers shall be controlled and marked in the same manner as prescribed for a finished classified document:

(i) Released by the originator outside the originating activity;

(ii) Retained more than 180 days from the date of origin;

(iii) Filed permanently.

(6) Information contained in unmarked records, or Presidential or related materials, and which pertain to the national defense or foreign relations of the U.S. and has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under this Order and is subject to its provisions regarding declassification.

§ 1312.9 Downgrading and declassification.

Classified information originated by OMB offices will be downgraded or declassified as soon as it no longer qualifies for continued protection under the provisions of the classification guides. Authority to downgrade or declassify OMB-originated information is granted to those authorized to classify (See § 1312.5). Additionally, the Associate Director for Administration is authorized to exercise downgrading and declassification actions up to and including the Top Secret level.

(a) Transferred material. Information which was originated by an agency that no longer exists, or that was received by OMB in conjunction with a transfer of functions, is deemed to be OMB-originated material. Information which has been transferred to another agency for storage purposes remains the responsibility of OMB.

(b) Periodic review of classified material. Each office possessing classified material will review that material on an annual basis or in conjunction with the transfer of files to non-current record storage and take action to downgrade or declassify all material no longer qualifying for continued protection at that level. All material transferred to non-current record storage must be properly marked with correct downgrade and declassification instructions.

§ 1312.10 Systematic review guidelines.

The EOP Security Officer will prepare and keep current such guidelines as are required by Executive Order 12958 for the downgrading and declassification of OMB material that is in the custody of the Archivist of the United States.

§ 1312.11 Challenges to classifications.

OMB employees are encouraged to familiarize themselves with the provisions of Executive Order 12958, April 20, 1995 and with OMB Manual Sections 1010, 1020, and 1030. Employees are also encouraged to question or to challenge those classifications they believe to be improper, unnecessary, or for an inappropriate time. Such questions or challenges may be addressed to the originator of the classification, unless the challenger desires to remain anonymous, in which case the question may be directed to the EOP Security Officer.

§ 1312.12 Security Program Review Committee.

The Associate Director for Administration will chair the OMB Security Program Review Committee, which will act on suggestions and complaints about the OMB security program.

Subpart B—Control and Accountability of Classified Information

§ 1312.21 Purpose and authority.

This subpart sets forth procedures for the receipt, storage, accountability, and transmission of classified information at the Office of Management and Budget. It is published under the authority of Executive Order 12958, April 20, 1995 as implemented by Directive No. 1, Information Security Oversight Office (60 FR 53492, October 13, 1995), and is applicable to all OMB employees.

§ 1312.22 Responsibilities.

The effective direction by supervisors and the alert performance of duty by employees will do much to ensure the adequate security of classified information in the possession of OMB offices. Each employee has a responsibility to protect and account for all classified information that he/she knows of within his/her area of responsibility.

Such information will be made available only to those persons who have an official need to know and who have been granted the appropriate security clearance. Particular care must be taken not to discuss classified information over unprotected communications circuits (to include intercom and closed-circuit TV), at non-

official functions, or at any time that it might be revealed to unauthorized persons. Classified information may only be entered into computer systems meeting the appropriate security criteria.

(a) EOP Security Officer. In cooperation with the Associate Director for Administration, the EOP Security Officer supervises the administration of this section. Specifically, he/she:

(1) Promotes the correct understanding of this section and insures that initial and annual briefings about security procedures are given to all new employees.

(2) Provides for periodic inspections of office areas and reviews of produced documents to ensure full compliance with OMB regulations and procedures.

(3) Takes prompt action to investigate alleged violations of security, and recommends appropriate administrative action with respect to violators.

(4) Supervises the annual inventories of Top Secret material.

(5) Ensures that containers used to store classified material meet the appropriate security standards and that combinations to security containers are changed as required.

(b) Heads of Offices. The head of each division or office is responsible for the administration of this section in his/her area. These responsibilities include:

(1) The appointment of accountability control clerks as prescribed in Part 1312.26 below.

(2) The maintenance of the prescribed control and accountability records for classified information within the office.

(3) Establishing internal procedures to ensure that classified material is properly safeguarded at all times.

§ 1312.23 Access to classified information.

Classified information may be made available to a person only when the possessor of the information establishes that the person has a valid ''need to know'' and the access is essential to the accomplishment of official government duties. The proposed recipient is eligible to receive classified information only after he/she has been granted a security clearance by the EOP Security Officer. Cover sheets will be used to protect classified documents from inadvertent disclosure while in use. An SF–703 will be used for Top Secret material; an SF–704 for Secret material, and an SF–705 for Confidential material. The cover sheet should be removed prior to placing the document in the files.

§ 1312.24 Access by historical researchers and former Presidential appointees.

(a) The requirements of Section 4.2(a)(3) of Executive Order 12958 may be waived for persons who are engaged in historical research projects, or who previously have occupied policy-making positions to which they were appointed by the President.

Waivers may be granted only if the Associate Director for Administration, in cooperation with the EOP Security Officer:

(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 the 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.

(b) In the instances described in paragraph (a) of this section, the Associate Director for Administration, in cooperation with the EOP Security Officer, will make a determination as to the trustworthiness of the requestor and will obtain written agreement from the requestor to safeguard the information to which access is given. He/She will also obtain written consent to the review by OMB of notes and manuscripts for the purpose of determining that no classified information is contained therein. Upon the completion of these steps, the material to be researched will be reviewed by the division/office of primary interest to ensure that access is granted only to material over which OMB has classification jurisdiction.

§ 1312.25 Storage.

All classified material in the possession of OMB will be stored in GSA-approved, steel safes possessing three-position, dial-type, changeable combination locks, or in vault-type rooms approved for Top Secret storage. Under the direction of the EOP Security Officer, combinations to safes used in the storage of classified material will be changed when the equipment is placed in use, whenever a person knowing the combination no longer requires access to it, whenever the combination has been subjected to possible compromise, whenever the equipment is taken out of service, or at least once a year. Knowledge of combinations will be limited to the minimum number of persons necessary, and records of combinations will be assigned a classification no lower than the highest level of classified information stored in the equipment concerned. An SF–700, Security Container Information, will be used in recording safe combinations. Standard Form-702, Security Container check sheet, will be posted to each safe and will be used to record opening, closing, and checking the container whenever it is used.

§ 1312.26 Control of secret and confidential material.

Classified material will be accounted for by the office having custody of the material. OMB For 87, Classified Document Control, will be used to establish accountability controls on all Secret material received or produced within OMB offices. No accountability controls are prescribed for Confidential material, but offices desiring to control and account for such material should use the procedures applicable to Secret material. Information classified by another agency shall not be disclosed without that agency's authorization.

(a) Accountability Control Clerks. Each division or office head will appoint one person as the Accountability Control Clerk (ACC). The ACC will be the focal point for the receipt, routing, accountability, dispatch, and declassification downgrading or destruction of all classified material in the possession of the office.

(b) OMB Form 87. One copy of OMB Form 87 will be attached to the document, and one copy retained in the accountability control file for each active document within the area of responsibility of the ACC. Downgrading or destruction actions, or, other actions removing the document from the responsibility of the ACC will be recorded on the OMB Form 87, and the form filed in an inactive file. Inactive control forms will be cut off annually, held for two additional years, then destroyed.

(c) Working Papers and Drafts. Working papers and drafts of classified documents will be protected according to their security classification, but will not be subject to accountability control unless they are forwarded outside of OMB.

(d) Typewriter Ribbons. Typewriter ribbons, cassettes, and other devices used in the production of classified material will be removed from the machine after each use and protected as classified material not subject to controls. Destruction of such materials will be as prescribed in Part 1312.29 below.

(e) Reproduction. Classified material will be reproduced only as required unless prohibited by the originator for the conduct of business and reproduced copies are subject to the same controls as are the original documents. Top

Secret material will be reproduced only with the written permission of the originating agency.

§ 1312.27 Top secret control.

The EOP Security Officer serves as the Top Secret Control Officer (TSCO) for OMB. He will be assisted by the Alternate TSCOs in each division/office Holding Top Secret material. The ATSCOs will be responsible for the accountability and custodianship of Top Secret material within their divisions/offices. The provisions of this section do not apply to special intelligence material, which will be processed as prescribed by the controlling agency.

(a) Procedures. All Top Secret material produced or received in OMB will be taken to the appropriate ATSCO for receipting, establishment of custodianship, issuance to the appropriate action officer, and, as appropriate, obtaining a receipt. Top Secret material in the custody of the TSCO or ATSCO will normally be segregated from other classified material and will be stored in a safe under his or her control. Such material will be returned to the appropriate ATSCO by action officers as soon as action is completed. OMB Form 87 will be used to establish custody, record distribution, routing, receipting and destruction of Top Secret material. Top Secret Access Record and Cover Sheet (Standard Form 703) will be attached to each Top Secret document while it is in the possession of OMB.

(b) Inventory. The Associate Director for Administration will notify each appropriate OMB office to conduct an inventory of its Top Secret material by May 1 each year. The head of each office will notify the EOP Security Officer when the inventory has been satisfactorily completed. Each Top Secret item will be examined to determine whether it can be downgraded or declassified, and the inventory will be adjusted accordingly. Discrepancies in the inventory, indicating loss or possible compromise, will be thoroughly investigated by the EOP Security Officer or by the Federal Bureau of Investigation, as appropriate. Each ATSCO will retain his/her division's inventory in accordance with the security procedures set forth herein.

§ 1312.28 Transmission of classified material.

Prior to the transmission of classified material to offices outside OMB, such material will be enclosed in opaque inner and outer covers or envelopes. The inner cover will be sealed and marked with the classification, and the address of the sender and of the addressee. The receipt for the document, OMB Form 87, (not required for Confidential material) will be attached to or placed within the inner envelope to be signed by the recipient and returned to the sender. Receipts will identify the sender, the addressee, and the document, and will contain no classified information. The outer cover or envelope will be sealed and addressed with no identification of its contents.

(a) Transmittal of Top Secret Material. The transmittal of Top Secret material shall be by personnel specifically designated by the EOP Security Officer, or by Department of State diplomatic pouch, by a messenger-courier system specifically created for that purpose. Alternatively, it shall be taken to the White House Situation Room for transmission over secure communications circuits.

(b) Transmittal of Secret Material. The transmittal of Secret material shall be as follows:

(1) Within and between the fifty States, the District of Columbia, and Puerto Rico: Use one of the authorized means for Top Secret material, or transmit by U.S. Postal Service express or registered mail.

(2) Other Areas. Use the same means authorized for Top Secret, or transmit by U.S. registered mail through Military Postal Service facilities.

(c) Transmittal of Confidential Material. As identified above, or transmit by U.S. Postal Service Certified, first class, or express mail service within and between the fifty States, the District of Columbia, and Puerto Rico.

(d) Transmittal Between OMB Offices and Within the EOP Complex. Classified material will normally be hand carried within and between offices in the Executive Office of the President complex by cleared OMB employees. Documents so carried must be protected by the appropriate cover sheet or outer envelope. Top Secret material will always be hand carried in this manner. Secret and Confidential material may be transmitted between offices in the EOP complex by preparing the material as indicated above (double envelope) and forwarding it by special messenger service provided by the messenger center. The messenger shall be advised that the material is classified. Receipts shall be obtained if Top Secret or Secret material is being transmitted outside of OMB. Classified material will never be transmitted in the Standard Messenger Envelope (SF Form 65), or by the Mail Stop system.

§ 1312.29 Destruction.

The destruction of classified material will be accomplished under the direction of the TSCO or the appropriate ATSCO, who will assure that proper accountability records are kept. Classified official record material will be processed to the OA Records Management Branch, NEOB Room 5208, in accordance with OMB Manual Section 540. Classified nonrecord material will be destroyed as soon as it becomes excess to the needs of the office. The following destruction methods are authorized:

(a) Shredding. Using the equipment approved for that purpose within OMB offices. Shredders will not accommodate typewriter ribbons or cassettes. Shredding is the only authorized means of Destroying Top Secret material.

(b) Burn Bag. Classified documents, cassettes, ribbons, and other materials at the Secret level or below, not suitable for shredding, may be destroyed by using burn bags, which can be obtained from the supply store. They will be disposed of as follows:

(1) OEOB: Unless on an approved list for pick-up of burn bags, all other burn bags should be delivered to Room 096 OEOB between 8:00 a.m. and 4:30 p.m. Burn bags are not to be left in hallways.

(2) NEOB: Hours for delivery of burn bag materials to the NEOB Loading Dock Shredder Room are Monday through Friday from 8:00 a.m. to 9:30 a.m.; 10:00 a.m. to 11:00 a.m.; 11:45 a.m. to 1:30 p.m. and 2:00 p.m. to 3:30 p.m. The phone number of the Shredder Room is 395–1593. In the event the Shredder Room is not manned, do not leave burn bags outside the Shredder Room as the security of that material may be compromised.

(3) Responsibility for the security of the burn bag remains with the OMB office until it is handed over to the authorized representative at the shredder room. Accountability records will be adjusted after the burn bags have been delivered. Destruction actions will be recorded on OMB Form 87 by the division TSCO or by the appropriate ATSCO at the time the destruction is accomplished or at the time the burn bag is delivered to the U.D. Officer.

(c) Technical Guidance. Technical guidance concerning appropriate methods, equipment, and standards for destruction of electronic classified media, processing equipment components and the like, may be obtained by submitting all pertinent information to NSA/CSS Directorate for Information Systems Security, Ft. Meade, Maryland 20755. Specifications concerning appropriate equipment and

standards for destruction of other storage media may be obtained from the General Services Administration.

§ 1312.30 Loss or possible compromise.

Any person who has knowledge of the loss or possible compromise of classified information shall immediately secure the material and then report the circumstances to the EOP Security Officer. The EOP Security Officer will immediately initiate an inquiry to determine the circumstances surrounding the loss or compromise for the purpose of taking corrective measures and/or instituting appropriate administrative, disciplinary, or legal action. The agency originating the information shall be notified of the loss or compromise so that the necessary damage assessment can be made.

§ 1312.31 Security violations.

(a) A security violation notice is issued by the United States Secret Service when an office/division fails to properly secure classified information. Upon discovery of an alleged security violation, the USSS implements their standard procedures which include the following actions:

(1) Preparation of a Record of Security Violation form;

(2) When a document is left on a desk or other unsecured area, the officer will remove the classified document(s) and deliver to the Uniformed Division's Control Center, and

(3) Where the alleged violation involves an open safe, the officer will remove one file bearing the highest classification level, annotate it with his or her name, badge number, date and time, and return the document to the safe, which will then be secured. A description of the document will be identified in the Record of Security Violations and a copy of the violation will be left in the safe.

(b) Office of Record. The EOP Security Office shall serve as the primary office of record for OMB security violations. Reports of violations will remain in the responsible individual's security file until one year after the individual departs the Executive Office of the President, at which time all violation reports will be destroyed.

(c) Compliance. All Office of Management and Budget employees will comply with this section. Additionally, personnel on detail or temporary duty will comply with this section, however, their parent agencies will be provided with a copy of any security violation incurred during their period of service to OMB.

(d) Responsibilities for Processing Security Violations. (1) EOP Security Officer. The EOP Security Officer shall provide OMB with assistance regarding Agency security violations. Upon receipt of a Record of Security Violation alleging a security violation, the EOP Security Officer shall:

(i) Prepare a memorandum to the immediate supervisor of the office/division responsible for the violation requesting that an inquiry be made into the incident. Attached to the memorandum will be a copy of the Record of Security Violation form. The receiving office/division will prepare a written report within five working days of its receipt of the Security Officer's memorandum.

(ii) Provide any assistance needed for the inquiry conducted by the office/division involved in the alleged violation.

(iii) Upon receipt of the report of inquiry from the responsible office/division, the EOP Security Officer will:

(A) Consult with the OMB Associate Director for Administration and the General Counsel;

(B) Determine if a damage assessment report is required. A damage assessment will be made by the agency originating the classified information, and will be prepared after it has been determined that the information was accessed without authorization; and

(C) Forward the report with a recommendation to the OMB General Counsel.

(2) Immediate Supervisors. Upon receipt of the EOP Security Officer's security violation memorandum, the immediate supervisor will make an inquiry into the alleged incident, and send a written report of inquiry to the EOP Security Officer. The inquiry should determine, and the related report should identify, at a minimum:

(i) Whether an actual security violation occurred,

(ii) The identity of the person(s) responsible; and

(iii) The probability of unauthorized access.

(3) Deputy Associate Directors (or the equivalent) will:

(i) Review and concur or comment on the written report; and

(ii) In conjunction with the immediate supervisor, determine what action will be taken to prevent, within their area of responsibility, a recurrence of the circumstances giving rise to the violation.

(e) Staff Penalties for OMB Security Violations. When assessing penalties in accordance with this section, only those violations occurring within the calendar year (beginning January 1) will be considered. However, reports of all previous violations remain in the security files. These are the standard violation penalties that will be imposed. At the discretion of the Director or his designee, greater or lesser penalties may be imposed based upon the circumstances giving rise to the violation, the immediate supervisor's report of inquiry, and the investigation and findings of the EOP Security Officer and/or the OMB Associate Director for Administration.

(1) *First violation.* (i) Written notification of the violation will be filed in the responsible individual's security file; and

(ii) The EOP Security Officer and/or the Associate Director for Administration will consult with the respective immediate supervisor, and the responsible individual will be advised of the penalties that may be applied should a second violation occur.

(2) *Second violation.* (i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director for Administration will consult with the respective Deputy Associate Director (or the equivalent) and immediate supervisor and the responsible individual who will be advised of the penalties that may be applied should a third violation occur; and

(iii) A letter of Warning will be placed in the Disciplinary Action file maintained by the Office of Administration, Human Resources Management Division.

(4) *Third violation.* (i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director for Administration will consult with the OMB Deputy Director, General Counsel, the respective Deputy Associate Director (or equivalent), and the immediate supervisor and the responsible individual who will be advised of the penalties that may be applied should a fourth violation occur; and

(iii) A Letter of Reprimand will be placed in the Disciplinary Action file maintained by the OA/HRMD.

(4) *Fourth Violation.* (i) Written notification of the violation will be filed in the responsible individual's security file;

(ii) The EOP Security Officer and/or the Associate Director for Administration will consult with the OMB Director, Deputy Director, General Counsel, the respective Deputy Associate Director (or the equivalent), and immediate supervisor;

(iii) The responsible individual may receive a suspension without pay for a period not to exceed 14 days; and

(iv) The responsible individual will be advised that future violations could result in the denial of access to classified material or other adverse actions as may be appropriate, including dismissal.

Subpart C—Mandatory Declassification Review

§ 1312.32 Purpose and authority.

Other government agencies, and individual members of the public, frequently request that classified information in OMB files be reviewed for possible declassification and release. This subpart prescribes the procedures for such review and subsequent release or denial. It is issued under the authority of Executive Order 12958, April 20, 1995, as implemented by Directive No. 1, Information Security Oversight Office (60 FR 53402, October 13, 1995).

§ 1312.33 Responsibility.

All requests for the mandatory declassification review of classified information in OMB files should be addressed to the Associate Director for Administration, who will acknowledge receipt of the request. When a request does not reasonably describe the information sought, the requester shall be notified that unless additional information is provided, or the scope of the request is narrowed, no further action will be taken. All requests will receive a response within 180 days of receipt of the request.

§ 1312.34 Information in the custody of OMB.

Information contained in OMB files and under the exclusive declassification jurisdiction of the office will be reviewed by the office of primary interest to determine whether, under the declassification provisions of the Order, the requested information may be declassified. If so, the information will be made available to the requestor unless withholding is otherwise warranted under applicable law. If the information may not be released, in whole or in part, the requestor shall be given a brief statement as to the reasons for denial, a notice of the right to appeal the determination to the Deputy Director, OMB, and a notice that such an appeal must be filed within 60 days in order to be considered.

§ 1312.35 Information classified by another agency.

When a request is received for information that was classified by another agency, the Associate Director for Administration will forward the request, along with any other related materials, to the appropriate agency for review and determination as to release. Recommendations as to release or denial may be made if appropriate. The requester will be notified of the referral, unless the receiving agency objects on the grounds that its association with the information requires protection.

§ 1312.36 Appeal procedure.

Appeals received as a result of a denial, see § 1312.34, will be routed to the Deputy Director who will take action as necessary to determine whether any part of the information may be declassified. If so, he will notify the requester of his determination and make that information available that is declassified and otherwise releasable. If continued classification is required, the requestor shall be notified by the Deputy Director of the reasons thereafter. Determinations on appeals will normally be made within 60 working days following receipt. If additional time is needed, the requestor will be notified and this reason given for the extension. The agency's decision can be appealed to the Interagency Security Classification Appeals Panel.

§ 1312.37 Fees.

There will normally be no fees charged for the mandatory review of classified material for declassification under this section.

[FR Doc. 96–23727 Filed 9–16–96; 8:45 am]

BILLING CODE 3110–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. NM–132, Notice No. SC–96–5–NM]

Special Conditions: Lockheed Martin Aerospace Corp. Model L382J Airplane

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed special conditions.

SUMMARY: This document proposes special conditions for the Lockheed Martin Aerospace Corp. Model L382J airplane. This airplane will have a novel or unusual design feature(s) associated with the installation of a dual head up display (HUD) to be used as a primary flight display (PFD) for all regimes of normal operation. The HUD will satisfy the basic requirements of § 25.1321 and serve as the primary source of flight director command information. This document contains the additional safety standards which the Administrator considers necessary to establish a level of safety equivalent to that established by the airworthiness standards of Part 25 of the federal Aviation Regulations (FAR).

DATES: Comments must be received on or before November 1, 1996.

ADDRESSES: Comments on this proposal may be mailed in duplicate to: Federal Aviation Administration, Office of the Assistant Chief Counsel, Attention: Rules Docket (ANM–7), Docket No. NM–132, 1601 Lind Avenue SW, Renton, Washington 98055–4056; or delivered in duplicate to the Office of the Assistant Chief Counsel at the above address. Comments must be marked: Docket No. NM–132. Comments may be inspected in the Rules Docket weekdays, except Federal holidays, between 7:30 a.m. and 4:00 p.m.

FOR FURTHER INFORMATION CONTACT: Dale Dunford, FAA, Flight Test and Systems Branch, ANM–111, Transport Standards Staff, Transport Airplane Directorate, Aircraft Certification Service, 1601 Lind Avenue SW, Renton, Washington, 98055–4056; telephone 206–227–2239.

SUPPLEMENTARY INFORMATION:

Comments Invited

Interested persons are invited to participate in the making of these proposed special conditions by submitting such written data, views, or augments as they may desire. Communications should identify the regulatory docket or notice number and be submitted in duplicate to the address specified above. All communications received on or before the closing date for comments will be considered by the Administrator before further rulemaking action on this proposal is taken. The proposals contained in this notice may be changed in light of the comments received. All comments received will be available, both before and after the closing date for comments, in the Rules Docket for examination by interested parties. A report summarizing each substantive public contact with FAA personnel concerning this rulemaking will be filed in the docket. Commenters wishing the FAA to acknowledge receipt of their comments submitted in response to this notice must include a self-addressed, stamped postcard on which the following statement is made: ''Comments to Docket No. NM–132.'' The postcard will be date/time stamped and returned to the commenter.