this area are not detected and an approved repair incorporated, impairment of the ability of the spar cap to carry design loads could result. If cracks are found, reduced inspection intervals are specified in the service letter with an appropriate crack length limitation to permit continued safe operation of the airplane until an approved repair is incorporated. In addition, incorporation of the approved repair is required if the crack limitation is exceeded. Accordingly, since the condition described herein is likely to exist or develop on other airplanes of the same type design, the FAA is issuing an AD applicable to Cessna 500, 501, 550 and 551 airplanes making compliance with the inspection procedures set forth in Cessna Citation Service Letters SL 57–2, Revision 2, and SL 550–57–1, Revision 1, mandatory.

Since a situation exists that requires the expeditious adoption of this regulation, it is found that notice and public procedure hereon are impracticable, and good cause exists for making this amendment effective in less than 30 days.

Adoption of the Amendment

In consideration of the foregoing, and pursuant to the authority delegated to me by the Administrator, § 39.13 of Part 39 of the Federal Aviation Regulations (14 CFR 39.13) is amended by adding the following new Airworthiness Directive:

Cessna: Applies to Models 500, 501, 550 and 551 airplanes with 600 or more hours time-in-service.

Compliance: Required as indicated unless already accomplished.

(A) Within the next 100 hours time-in-service after the effective date of this AD and thereafter within each 600 hours time in service until the number of landings or time-in-service threshold for dye penetrant inspection in Table I is reached, visually inspect the upper and lower spar cap stems at Wing Station 37.0 in the areas specified in Cessna Citation Service Letter SL 57–2, Revision 2, dated May 1, 1979, or SL 550–57–1, Revision 1, dated May 1, 1979, as applicable for cracks and/or:

(B) Upon reaching or if at or beyond the dye penetrant inspection threshold specified in Table I, within 100 hours time-in-service or 100 landings, whichever occurs first, and thereafter within 600 hours time-in-service or 600 landings, whichever occurs first, dye penetrant inspect the upper and lower spar cap stem at Wing Station 37.0 in the areas specified in Cessna Citation Service Letter SL 57–2, Revision 2, dated May 1, 1979, or SL 550–57–1, Revision 1, dated May 1, 1979, as applicable, for cracks.

Table I

Model	Serial Nos.	Dye penetrant inspection threshold (Landings or time-in-service-hrs)
500	500-001 thru 500-349	4300
	500-350 and on	1300
501	501-001 and on	1300
550	550-001 and on	4300
551	551-001 and on	4300

(C) If, as a result of any inspection required by Paragraph A) or B) a crack of less than .3 inches in length is found in the upper spar cap stem, reduce the dye penetrant inspection interval on this spar cap to 200 landings or 200 hours time-in-service, whichever occurs first.

(D) If, as a result of any inspection required by Paragraph A) or B) a crack of less than .3 inches in length is found in the lower spar cap stem, reduce the dye penetrant inspection interval on this spar cap to 100 landings or 100 hours time-in-service, whichever occurs first.

Note.—The FAA encouraged compliance with the manufacturer's request that all cracks be reported to the Cessna Customer Service Department.

(E) If, as a result of any inspection required by Paragraph A), B), C) or D), a crack of .3 inches in length or longer is found in either spar cap, prior to further flight, repair or modify the wing in accordance with instructions obtained from Cessna Aircraft Company, Jet Marketing Division, Customer Service, P.O. Box 7706, Wichita, Kansas 67277.

(F) The time-in-service for initial and between repetitive inspections required herein may be adjusted up to 10 hours to facilitate accomplishing them concurrent with other scheduled maintenance on the airplane.

(G) Aircraft may be flown in accordance with Federal Aviation Regulation 21.197 to a location where this AD can be accomplished.

(H) Any equivalent method of compliance with this AD must be approved by the Chief, Engineering and Manufacturing Branch, FAA, Central Region.

Cessna Citation Service Letter SL 57–2, Revision 2 dated May 1, 1979, covers the subject matter of this AD.

This Amendment becomes effective June 21, 1979.

Secs. 313(a), 601 and 603, Federal Aviation Act of 1958, as amended, (49 U.S.C. 1354(a), and 1423); Sec. 6(c), Department of Transportation Act (49 U.S.C. 1655(c)); and Sec. 11.89 of the Federal Aviation Regulations (14 CFR 11.89).

Note.—The FAA has determined that this document involves a regulation which is not significant under Executive Order 12044, as implemented by Department of Transportation Regulatory Policies and Procedures (44 FR 11034; February 26, 1979). A copy of the final evaluation prepared for this document is contained in the docket. A copy of it may be obtained by writing to FAA, Office of the Regional Counsel, Room 1558, 601 East 12th Street, Kansas City, Missouri 64106.

Issued in Kansas City, Missouri on June 4, 1979.

C. R. Melugin, Jr.,

Director, Central Region.

[FR Doc. 79-18647 Filed 6-15-79; 8:45 am]

BILLING CODE 4910-13-M

14 CFR Part 39

[Docket No. 79-SO-42; Amdt. 39-3490]

Airworthiness Directives; Piper Model PA-44-180 Series Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This amendment adopts a new Airworthiness Directive (AD) which requires the replacement, on both engines, of the engine primer lines on certain Piper PA–44–180 airplanes. This AD is prompted by reports of broken primer lines and cracked or broken fittings that result in fuel leakage creating a potential fire hazard.

DATE: Effective June 21, 1979.

Compliance required as indicated.

ADDRESSES:

The applicable service bulletin may be obtained from Piper Aircraft Corporation, 820 East Bald Eagle Street, Lock Haven, Pennsylvania 17745.

A copy of the Service Bulletin is contained in the AD Docket File and may be examined in Room 275, Federal Aviation Administration, Southern Region, 3400 Whipple Street, East Point, Georgia.

FOR FURTHER INFORMATION CONTACT:

Gil Carter, ASO–214, Propulsion Section, Engineering and Manufacturing Branch, FAA, Southern Region, P.O. Box 20636, Atlanta, Georgia 30320, telephone (404) 763–7435.

SUPPLEMENTARY INFORMATION: There have been reports of broken primer lines and cracked and broken fittings on Piper Model PA–44–180 series airplanes which result in fuel leakage into the engine compartment near the engine exhaust manifolds thus creating a potential fire hazard. Since this condition is likely to exist or develop in other airplanes of the same type design, an Airworthiness Directive is being issued which requires the installation of new engines primer lines on certain Piper PA–44–180 airplanes.

Since a situation exists that requires immediate adoption of this regulation, it is found that notice and public procedure hereon are impracticable, and good cause exists for making this amendment effective in less than 30 days.

Adoption of the Amendment

Accordingly, pursuant to the authority delegated to me by the Administrator, § 39.13 of Part 39 of the Federal Aviation Regulation (14 CFR 39.13) is amended by adding the following new Airworthiness Directive:

Piper Aircraft Corporation: Applies to Model PA-44-180, serial numbers 44-7995001 through 44-7995190 airplanes certificated in all categories.

Compliance is required within the next 25 hours' time in service after the effective date of this AD or within 30 days after the effective date of this AD, whichever occurs first, unless already accomplished.

To prevent a potential fire hazard due to fuel leakage from failed primer lines and cracked and broken fittings, accomplish the following on both engines:

(a) Install the fuel primer modification kit, Piper Part Number 763 908V in accordance with Piper Service Bulletin 634 dated December 28, 1978, or later revision approved by the Chief, Engineering and Manufacturing Branch, Federal Aviation Administration, Southern Region.

(b) Make an appropriate maintenance record entry.

An equivalent method of compliance may be approved by the Chief, Engineering and Manufacturing Branch, Federal Aviation Administration, Southern Region.

This amendment becomes effective June 21, 1979.

(Secs. 313(a), 601, and 603, Federal Aviation Act of 1958, as amended (49 U.S.C. 1354(a), 1421, and 1423); Sec. 6(c), Department of Transportation Act (49 U.S.C. 1655(c)); 14 CFR 11.89.)

Issued in East Point, Georgia, on June 4, 1979.

George R. La Caille,

Acting Director, Southern Region.

[FR Doc. 79-18649 Filed 6-15-79; 8:45 am]

BILLING CODE 4910-13-M

14 CFR Part 71

[Airspace Docket No. 79-SO-26]

Designation of Federal Airways, Area Low Routes, Controlled Airspace, and Reporting Points; Designation of Transition Area, Springfield, Kentucky

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This Rule designates the Springfield, KY, Transition Area. It will afford protected airspace for IFR aircraft using the new public use instrument approach procedure established for that airport by lowering the base of controlled airspace from 1200 to 700 feet AGL.

EFFECTIVE DATE: August 9, 1979.

ADDRESS: Federal Aviation Administration, Chief, Air Traffic Division, P.O. Box 20636, Atlanta, Georgia 30320.

FOR FURTHER INFORMATION CONTACT: Gerald S. Collins, Airspace and Procedures Branch, Federal Aviation Administration, P.O. Box 20636, Atlanta, Georgia 30320; telephone: 404-763-7646.

SUPPLEMENTARY INFORMATION: An instrument approach procedure has been developed to enable aircraft operating in Instrument Flight Rule (IFR) weather conditions to conduct a safe approach for landing at Springfield-Lebanon Airport, KY. Consequently, adequate controlled airspace is required to provide airspace protection for IFR use of the procedure. This action is designed to meet that requirement as well as change the operating status of Springfield-Lebanon Airport from VFR to IFR. Notice to this effect was published in the **Federal Register** Thursday, April 19, 1979 (44 FR 23259). No objections were received from this Notice.

Adoption of the Amendment

Accordingly, Subpart G, § 71.181 (44 FR 442) of Part 71 of the Federal Aviation Regulations (14 CFR 71) is amended, effective 0901 GMT, August 9, 1979, by adding the following:

Springfield, Kentucky

That airspace extending upward from 700 feet above the surface within a 6.5-mile radius of the Lebanon-Springfield Airport (Latitude 37°38'02"N., Longitude 85°14'30"W.); within 3 miles either side of the New Hope, Kentucky, VORTAC, 089° radial extending from the 6.5-mile radius area to 14 miles east of the VORTAC.

(Sec. 307(a) of the Federal Aviation Act of 1958, as amended (49 U.S.C. 1348(a)) and sec. 6(c) of the Department of Transportation Act (49 U.S.C. 1655(c)).)

Note.—The Federal Aviation Administration has determined that this document involves a regulation which is not significant under Executive Order 12044, as implemented by DOT Regulatory Policies and Procedures (44 FR 11034, February 26, 1979). Since this regulatory action involves an established body of technical requirements for which frequent and routine amendments are necessary to keep them operationally current and promote safe flight operations, the anticipated impact is so minimal that this action does not warrant preparation of a regulatory evaluation.

Issued in East Point, Georgia, on June 8, 1979.

Lonnie D. Parrish,

Acting Director, Southern Region.

[FR Doc. 79-18650 Filed 6-15-79; 8:45 am]

BILLING CODE 4910-13-M

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

14 CFR Part 1203

Information Security Program

AGENCY: National Aeronautics and Space Administration.

ACTION: Final rule.

SUMMARY: This amendment is necessary to comply with the provisions of Executive Order 12065, "National Security Information." This amendment sets forth guides and guidelines for classifying, declassifying and downgrading information and material under the NASA Information Security Program. This amendment also assigns responsibilities for the management and direction of the Program.

DATE: June 18, 1979.

ADDRESS: Director, Security Division, National Aeronautics and Space Administration, Washington, DC 20546.

FOR FURTHER INFORMATION CONTACT: Arnold K. Daue, telephone (202) 755-3400.

SUPPLEMENTARY INFORMATION: This regulation involves national security and is exempt from the procedures of 5 U.S.C. 553.

1. 14 CFR Part 1203 is amended by revising Subparts A through E and by adding new Subparts F and G.

PART 1203—INFORMATION SECURITY PROGRAM

Subpart A—Scope

Sec.

1203.100 Legal basis.
1203.101 Other applicable NASA regulations.

Subpart B—NASA Information Security Program

1203.200 Background and discussion.
1203.201 Information security objectives.
1203.202 Responsibilities.
1203.203 Degree of protection.

Subpart C—Classification Principles and Considerations

1203.300 General.
1203.301 Identification of information requiring protection.
1203.302 Combination, interrelation or compilation.
1203.303 Dissemination considerations.
1203.304 Internal effect.
1203.305 Restricted data.

Subpart D—Guides for Original Classification

1203.400 Specific classifying guidance.
1203.401 Effect of open publication.
1203.402 Classifying material other than documentation.
1203.403 State-of-the-art and intelligence.
1203.404 Handling of unprocessed data.

Sec.

1203.405 Proprietary information.
1203.406 Additional classification factors.
1203.407 Duration of classification.
1203.408 Assistance by installation security classification officers.
1203.409 Exceptional cases.
1203.410 Identification and marking.
1203.411 Prohibitions.
1203.412 Classification guides.

Subpart E—Derivative Classification

1203.500 Use of derivative classification.
1203.501 Applying derivative classification markings.

Subpart F—Declassification and Downgrading

1203.600 Policy.
1203.601 Responsibilities.
1203.602 Public interest vs. declassification.
1203.603 Systematic review for declassification.
1203.604 Mandatory review for declassification.

Subpart G—Foreign Government Information

1203.700 Identification.
1203.701 Classification.
1203.702 Duration of classification.
1203.703 Declassification.

* * * * *

Authority: 42 U.S.C. 2451 et seq. and E. O. 12065.

Subpart A—Scope.

§ 1203.100 Legal basis.

(a) *E.O. 12065.* The responsibilities and authority of the Administrator of NASA with respect to the original classification of official information or material requiring protection against unauthorized disclosure in the interest of national defense or foreign relations of the United States (hereinafter collectively termed "national security"), and the standards for such classification, are established by Executive Order 12065 (43 FR 28949) and the Information Security Oversight Office Directive No. 1, September 29, 1978.

(b) *E.O. 10865.* Executive Order 10865 (24 FR 1583) requires the Administrator to prescribe by regulation such specific requirements, restrictions and other safeguards as the Administrator may consider necessary to protect:

(1) Releases of classified information to or within United States industry that relate to contracts with NASA; and

(2) Other releases of classified information to industry that NASA has responsibility for safeguarding.

(c) *The National Aeronautics and Space Act.* (1) Section 304(a) of the National Aeronautics and Space Act of 1958, as amended (42 U.S.C. 2451 et seq.), states in part: "The Administrator shall establish such security requirements, restrictions, and safeguards as he deems necessary in the interest of the national security * * *"

(2) Section 303 of the Act states: "Information obtained or developed by the Administrator in the performance of his functions under this Act shall be made available for public inspection, except (i) information authorized or required by Federal Statute to be withheld, and (ii) information classified to protect the national security: *Provided*, That nothing in this Act shall authorize the withholding of information by the Administrator from the duly authorized committees of the Congress."

§ 1203.101 Other applicable NASA regulations.

(a) Subpart H of this Part, "Delegation of Authority to Make Determinations in Original Security Classification Matters."

(b) Subpart I of this Part, "NASA Information Security Program Committee."

(c) NASA Handbook 1620.3, "NASA Physical Security Handbook."

Subpart B—NASA Information Security Program

§ 1203.200 Background and discussion.

(a) In establishing a civilian space program, the Congress required NASA to "provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof," and for the withholding from public inspection of that information that is classified to protect the national security.

(b) To balance the public's interest in access to Government information with the need to protect certain national security information from unauthorized disclosure, Executive Order 12065 was promulgated. It designates the National Aeronautics and Space Administration as having certain responsibility for matters pertaining to national security, and confers on the Administrator of NASA, or such responsible officers or employees as the Administrator may designate, the authority for original classification of official information or material which requires protection in the interest of national security. It also provides for:

(1) Basic classification, downgrading and declassification guidelines;

(2) The issuance of directives prescribing the procedures to be followed in safeguarding classified information or material;

(3) A monitoring system to ensure the effectiveness of the Order;

(4) Appropriate administrative sanctions against officers and employees of the United States Government who are found to be in violation of the Order or implementing directive; and

(5) Classification prohibitions as discussed in § 1203.411.

(c) Executive Order 12065 requires the timely identification and protection of that NASA information the disclosure of which would be contrary to the best interest of national security. Accordingly, the determination in each case must be based on a judgment as to whether disclosure of information could reasonably be expected to result in identifiable damage to the national security.

§ 1203.201 Information security objectives.

The objectives of the NASA Information Security Program are to:

(a) Ensure that information is classified only when a sound basis exists for such classification and only for such period as is necessary.

(b) Prevent both the unwarranted classification and the overclassification of NASA information.

(c) Ensure the greatest practicable uniformity within NASA in the classification of information.

(d) Ensure effective coordination and reasonable uniformity with other Government departments and agencies, particularly in areas where there is an interchange of information, techniques or hardware.

(e) Provide a timely and effective means for downgrading or declassifying information when the circumstances necessitating the original classification change or no longer exist.

§ 1203.202 Responsibilities.

(a) The Chairperson, NASA Information Security Program Committee (Subpart I of this Part), is responsible for:

(1) Directing the NASA Information Security Program in accordance with NASA policies and objectives and applicable laws and regulations.

(2) Ensuring effective compliance with and implementation of Executive Order 12065 and the Information Security Oversight Office Directive No. 1 relating to security classification matters.

(3) Reviewing, in consultation with the NASA Information Security Program Committee, questions, suggestions, appeals and compliance concerning the NASA Information Security Program and making determinations concerning them.

(4) Coordinating NASA security classification matters with NASA installations, the Department of Defense, the Department of Energy and other Government agencies.

(5) Issuing Security Classification Guides for NASA programs and projects.

(6) Developing, maintaining and recommending to the Administrator guidelines for the systematic review covering 20-year old classified information under NASA's jurisdiction.

(7) Reviewing and coordinating with appropriate offices all appeals of denials of requests for records under sections 552 and 552a of Title 5, United States Code (Freedom of Information and Privacy Acts) when the denials are based on the records continued classification.

(8) Recommending to the Administrator appropriate administrative action to correct abuse or violations of any provision of the NASA Information Security Program, including notifications by warning letter, formal reprimand and to the extent permitted by law, suspension without pay and removal.

(b) All NASA employees are responsible for bringing to the attention of the Chairperson of the NASA Information Security Program Committee any information security problems in need of resolution, any areas of interest wherein information security guidance is lacking, and any other matters likely to impede achievement of the objectives prescribed herein.

(c) Each NASA official to whom the authority for original classification is delegated shall be accountable for the propriety of each classification (see Subpart H) and is responsible for:

(1) Ensuring that classification determinations are consistent with the policy and objectives prescribed above, and other applicable guidelines.

(2) Bringing to the attention of the Chairperson, NASA Information Security Program Committee, for resolution, any disagreement with classification determinations made by other NASA officials.

(3) Ensuring that information and material which no longer requires its present level of protection is promptly downgraded or declassified in accordance with applicable guidelines.

(d) Other Officials-in-Charge of Headquarters Offices are responsible for:

(1) Ensuring that classified information or material prepared within their respective offices is appropriately marked.

(2) Ensuring that material proposed for public release is reviewed to eliminate classified information.

(e) Directors of Field Installations and, for Headquarters, the Director, Headquarters Administration Division, are responsible for:

(1) Developing proposed Security Classification Guides.

(2) Ensuring that classified information or material prepared in their respective installations is appropriately marked.

(3) Ensuring that material proposed for public release is reviewed to eliminate classified information.

(4) Designating Security Classification Officers at their respective installations, to whom the responsibilities listed in paragraphs (e) (1), (2), and (3) of this section may be reassigned.

(f) The NASA Security Classification Manager, Security Division, NASA Headquarters, who serves as a member and Executive Secretary of the NASA Information Security Program Committee, is responsible for the NASA-wide coordination of security classification matters.

(g) The Director of Security is responsible for establishing procedures for the safeguarding of classified information or material (e.g., accountability, control, access, storage, transmission, marking, etc.) and for ensuring that such procedures are systematically reviewed and those which are duplicative or unnecessary are eliminated.

§ 1203.203 Degree of Protection.

(a) *General.* Upon determination that information or material must be classified, the degree of protection (security classification) commensurate with the sensitivity of the information must be determined. The lowest category of classification necessary to provide the appropriate degree of protection should be assigned. If the classifier has a reasonable doubt as to which security classification category is appropriate, or whether the material should be classified at all, the least restrictive designation should be used, or the information should not be classified.

(b) *Authorized Categories of Classification.* The three categories of classification, as authorized and defined in Executive Order 12065 are set out below. No other restrictive markings are authorized to be placed on NASA classified documents or materials except as expressely provided by statute or by NASA Directives.

(1) *Top Secret.* Top Secret is the designation applied to information or material the unathorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret.* Secret is the designation applied to information or material the unathorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological develpments relating to national security.

(3) *Confidential.* Confidential is the designation applied to that information or material the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security.

Subpart C—Classification Principles and Considerations

§ 1203.300 General.

In general, the types of NASA-generated information and material requiring protection in the interest of national security lie in the areas of applied research, technology or operations.

§ 1203.301 Identification of information requiring protection.

Classifiers shall identify the level of classification of each classified portion of a document (including subject and titles), and those portions that are not classified.

§ 1203.302 Combination, interrelation or compilation.

An interrelationship of individual items, classified or unclassified, may result in a combined item requiring a higher classification than that of any of the individual items. Compilations of unclassified information are considered unclassified unless some additional significant factor is added in the process of compilation. For example: (a) The

way unclassified information is compiled may be classified; (b) the fact that the information is complete for its intended purpose may be classified; or (c) the fact the compilation represents an official evaluation may be classified. In these cases, the compilations would be classified.

§ 1203.303 Dissemination considerations.

The degree of intended dissemination, use of the information and whether the end purpose to be served renders effective security control impractical are considerations during the classification process. These factors do not necessarily preclude classification, but must be considered in order not to impose security controls which are impractical to enforce.

§ 1203.304 Internal effect.

The effect of security protection on program progess and cost and on other functional activities of NASA should be considered. Impeditive effects and added costs inherent in a security classification must be assessed in light of the detrimental effects on the national security interests which would result from failure to classify.

§ 1203.305 Restricted data.

Restricted Data or Formerly Restricted Data is so classified when originated, as required by the Atomic Energy Act of 1954, as amended. Specific guidance for the classification of Restricted Data is provided in "Classification Guides" published by the Department of Energy.

Subpart D—Guides for Original Classification

§ 1203.400 Specific classifying guidance.

Technological and operational information and material, and in some exceptional cases scientific information, falling within any one or more of the following categories must be classified if its unauthorized disclosure could reasonably be expected to cause identifiable damage to the national security. In cases where it is believed that a contrary course of action would better serve the national interests, the matter should be referred to the Chairperson, NASA Information Security Program Committee, for a determination. It is not intended that this list be exclusive; original classifiers are responsible for initially classifying any other type of information which, in their judgment, requires protection within the intent of Executive Order 12065:

(a) Information which provides the United States, in comparison with other nations, with a significant scientific, engineering, technical, operational, intelligence, strategic, tactical or economic advantage related to national security.

(b) Information which if disclosed would significantly diminish the technological lead of the United States in any military system, subsystem or component thereof, resulting in identifiable damage to such a system, subsystem or component thereof.

(c) Scientific or technological information in an area where an advanced military application that would in itself be classified is foreseen during exploratory development.

(d) Information which, if known, would: (1) Provide a foreign nation with an insight into the defense application or the war or defense plans or posture of the United States;

(2) Allow a foreign nation to develop, improve or refine a similar item of defense application;

(3) Provide a foreign nation with a base upon which to develop effective countermeasures;

(4) Weaken or nullify the effectiveness of a defense or military plan, operation, project, weapon system or activity which is vital to the national security.

(e) Information or material which is important to the national security of the United States in relation to other nations when there is sound reason to believe that those nations are unaware that the United States has or is capable of obtaining the information or material; i.e., through intelligence activities, sources, or methods.

(f) Information which if disclosed could be exploited in a manner prejudicial to the national security posture of the United States by discrediting its technological power, capability or intentions.

(g) Information which reveals an unusually significant scientific or technological "breakthrough" which there is sound reason to believe is not known to or within the state-of-the-art capability of other nations. If the "breakthrough" supplies the United States with an important advantage of a technological nature, classification also would be appropriate if the potential application of the information, although not specifically visualized, would afford the United States a significant national security advantage in terms of technological lead time or an economic advantage relating to national security.

(h) Information of such nature that an unfriendly government in possession of it would be expected to use it for purposes prejudicial to U.S. national security and which, if classified, could not be obtained by an unfriendly power without a considerable expenditure of resources.

(i) Information which if disclosed to a foreign government would enhance its military research and development programs to the detriment of U.S. counterpart or competitive programs.

(j) Operational information pertaining to the command and control of space vehicles, the possession of which would facilitate malicious interference with U.S. space mission, that might result in identifiable damage to the national security.

(k) Information which if disclosed could jeopardize the foreign relations or activities of the United States; for example, the premature or unauthorized release of information relating to the subject matter of international negotiations, foreign government information or information regarding the placement or withdrawal of NASA tracking stations on foreign territory.

(l) United States Government programs for safeguarding nuclear materials or facilities.

(m) Other categories of information which are related to national security and which require protection against unauthorized disclosure as may be determined by the Administrator. The Chairperson, NASA Information Security Program Committee, will promptly inform the Director, Information Security Oversight Office, General Services Administration (GSA) of such determinations.

§ 1203.401 Effect of open publication.

Public disclosure, regardless of source or form, of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosure requires an immediate reevaluation to determine whether the information has been compromised to the extent that downgrading or declassification is indicated. Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. In these cases, if a release were made or authorized by an official Government source, classification of clearly identified items may no longer be warranted. Questions as to the propriety of continued classification should be referred to the Chairperson, NASA Information Security Program Committee.

§ 1203.402 Classifying material other than documentation.

Items of equipment or other physical objects may be classified only where classified information may be derived by visual observation of internal or external appearance, structure, operation, test, application or use. The overall classification assigned to equipment or objects shall be at least as high as the highest classification of any of the items of information which may be revealed by the equipment or objects, but may be higher if the classifying authority determines that the sum of classified or unclassified information warrants such higher classification. In every instance where classification of an item of equipment or object is determined to be warranted, such determination must be based on a finding that there is at least one aspect of the item or object which requires protection. If mere knowledge of the existence of the equipment or object would compromise or nullify the reason or justification for its classification, the fact of its existence should be classified.

§ 1203.403 State-of-the-art and intelligence.

A logical approach to classification requires consideration of the extent to which the same or similar information available from intelligence sources is known or is available to others. It is also important to consider whether it is known publicly, either domestically or internationally, that the United States has the information or even is interested in the subject matter. The known state-of-the-art in other nations is an additional substantive factor requiring consideration.

§ 1203.404 Handling of unprocessed data.

It is the usual practice to withhold the release of raw scientific data received from spacecraft until it can be calibrated, correlated and properly interpreted by the experimenter under the monitorship of the cognizant NASA office. During this process, the data are withheld through administrative measures, and it is not necessary to resort to security classification to prevent premature release. However, if at any time during the processing of raw data it becomes apparent that the results require protection under the criteria set forth in this Subpart D, it is the responsibility of the cognizant NASA office to obtain the appropriate security classification.

§ 1203.405 Proprietary information.

Proprietary information made available to NASA is subject to examination for classification purposes under the criteria set forth in this Subpart D. Where the information is in the form of a proposal and accepted by NASA for support, it should be categorized in accordance with the criteria of § 1203.400. If NASA does not support the proposal but believes that security classification would be appropriate under the criteria of § 1203.400 if it were under Government jurisdiction, the contractor should be advised of the reasons why safeguarding would be appropriate, unless security considerations preclude release of the explanation to the contractor. NASA should identify the Government department, agency or activity whose national security interests might be involved and the contractor should be instructed to protect the proposal as though classified pending further advisory classification opinion by the Government activity whose interests are involved. If such a Government activity cannot be identified, the contractor should be advised that the proposal is not under NASA jurisdiction for classification purposes, and that the information should be sent, under proper safeguards, to the Director, Information Security Oversight Office, General Services Administration, Washington, D.C. 20405, for a determination.

§ 1203.406 Additional classification factors.

In determining the appropriate classification category, the following additional factors should be considered:

(a) *Uniformity Within Government Activities.* The effect classification will have on technological programs of other Government departments and agencies should be considered. Classification of official information must be reasonably uniform within the Government.

(b) *Applicability of Classification Directives of Other Government Agencies.* It is necessary to determine whether authoritative classification guidance exists elsewhere for the information under consideration which would make it necessary to assign a higher classification than that indicated by the applicable NASA guidance. Generally, the classification by NASA should not be higher than that of equivalent information in other departments or agencies of the Government.

§ 1203.407 Duration of classification.

(a) Except as permitted in paragraph (b) of this section, each original classification authority shall set a date or event for automatic declassification no more than six years later.

(b) Only officials with Top Secret classification authority listed in Subpart H may classify information for more than six years from the date of the original classification. This authority shall be used sparingly. In such cases, a declassification date or event, or a date for review, shall be set. This date or event shall be as early as national security permits and shall be no more than 20 years after original classification except as provided under the provisions of § 1203.603.

§ 1203.408 Assistance by installation security classification officers.

Installation Security Classification Officers, as the installation point-of-contact, will assist installation personnel in:

(a) Interpreting security classification guides and classification assignments for the installation.

(b) Answering questions and considering suggestions concerning security classification matters.

(c) Ensuring a continuing review of classified information for the purpose of declassifying or downgrading in accordance with Subpart E of this part.

(d) Reviewing and approving, as the representative of the contracting officer, the DD Form 254, Contract Security Classification Specification, issued to contractors by the installation.

§ 1203.409 Exceptional cases.

(a) In those cases where a person not authorized to classify information orginates or develops information which is believed to require classification, that person should safeguard the material as though it were classified until it has been evaluated and a decision made by an appropriate classifying authority. For NASA employees the classifying authority is normally the Installation Security Classification Officer. Persons other than NASA employees should forward, under appropriate safeguards, material in which NASA has primary interest to the NASA Information Security Program Committee, Security Division, Washington, DC 20546 for a classification determination.

(b) Information in which NASA does not have primary interest shall be returned promptly, under appropriate safeguards, to the sender in accordance with § 1203.405.

(c) Material received from another agency for a NASA security classification determination shall be processed within 30 days. If a classification cannot be determined during that period, the material shall be

sent, under appropriate safeguards, to the Director, Information Security Oversight Office, GSA, for a determination.

§ 1203.410 Prohibitions.

(a) Classification may not be used to conceal violations of law, inefficiency of administrative error; to prevent embarrassment to a person, organization or agency; or to restrain competition.

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

(c) A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Part 1203 until and unless the Government acquires a proprietary interest in the product. This Part 1203 does not affect the provisions of the Patent Secrecy Act of 1952 (35 U.S.C. 181–188).

(d) References to classified documents that do not disclose classified information may not be classified or used as a basis for classification.

(e) Classification may not be used to limit dissemination of information that is not classifiable under the provisions of this Part 1203 or to prevent or delay the public release of such information.

(f) No document originated on or after December 1, 1978, may be classified *after* NASA has received a request for the document under the Freedom of Information Act or the mandatory review provisions of this Part 1203, unless such classification is consistent with this Part 1203 and is authorized by the Administrator or Deputy Administrator. Documents originated before December 1, 1978, and subject to such a request may not be classified unless such classification is consistent with this Part 1203 and is authorized by the Chairperson, NASA Information Security Program Committee, or by an official with Top Secret classification authority. Classification authority under this provision shall be exercised personally, on a document-by-document basis.

(g) Classification may not be restored to documents already declassified and released to the public.

§ 1203.412 Classification guides.

(a) *General.* A classification guide, based upon classification determinations made by appropriate program and classification authorities, shall be issued for each classified system, program or project. Classification guides shall:

(1) Identify the information elements to be protected, using categorization and subcategorization to the extent necessary to ensure that the information involved can be readily and uniformly identified.

(2) State which of the classification designations (i.e., Top Secret, Secret or Confidential) apply to the identified information elements.

(3) State the duration of each such specified classification in terms of a period of time or future event. When such duration is to exceed six years, the decision must be made by an original Top Secret classification authority and the specific reason for prolonging classification beyond the six-year period shall be provided in the guidance in accordance with the provisions of § 1203.407. If the reason for prolonging classification beyond six years would be the only cause for classification of the guide or would raise the level of the classification of the guide, it need by recorded only on the record copy of the guide.

(4) Indicate specifically, that the designations, time limits, markings and other requirements of Executive Order 12065 are to be applied to information classified pursuant to the guide.

(5) Be approved personally and in writing by an official with original Top Secret classification authority; the identity of the official will be shown on the guide. Such approval constitutes an original classification decision. Normally, all guides will be approved by the Chairperson, NASA Information Security Program Committee, whose office will maintain a list of all classification guides in current use.

(b) *Review of Classification Guides.* Classification guides shall be reviewed by the originator for currency and accuracy not less than once every two years. Changes shall be in strict conformance with the provisions of this Part 1203 and shall be issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review.

Subpart E—Derivative Classification.

§ 1203.500 Use of derivative classification.

Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, generate in new form or respond to information which is already classified or those who apply markings in accordance with a security classification guide issued by an authorized classifier. Persons who apply derivative classifications shall take care to determine whether their paraphrasing, restating or summarizing of classified information has removed all or part of the basis for classification.

§ 1203.501 Applying derivative classification markings.

Persons who apply derivative classification markings shall:

(a) Respect original classification decisions;

(b) Verify the information's current level of classification so far as practicable before applying the markings; and

(c) Carry forward to any newly created documents the assigned dates or events for declassification or review and any additional authorized markings. Where checks with originators or other appropriate inquiries show that no classification or a lower classification than originally assigned is appropriate, the derivative document shall be issued unclassified or shall be marked accordingly.

Subpart F—Declassification and Downgrading

§ 1203.600 Policy.

Declassification of classified information shall be given emphasis comparable to that accorded classification. Information classified pursuant to Executive Order 12065 and prior orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or on the occurrence of a declassification event. When information is reviewed for declassification pursuant to this Part 1203 or the Freedom of Information Act, it shall be declassified unless the classification authority established pursuant to Subpart H determines that the information continues to meet the classification guidelines prescribed in § 1203.400 despite the passage of time.

§ 1203.601 Responsibilities.

Officials authorized original classification authority may declassify or downgrade information that is subject to the final classification jurisdiction of NASA and shall take such action in accordance with the provisions of this Subpart F.

§ 1203.602 Public interest vs. declassification.

It is presumed that information which continues to meet the classification requirements in § 1203.407(b) requires continued protection. In rare 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 concerning NASA information, they shall be referred to the Administrator; the Chairperson, NASA Information Security Program Committee; an official with Top Secret classification authority; or, in the case of Presidential papers, the Archivist of the United States. That official, after appropriate consultation with other agencies or Government components, will determine whether the public interest in disclosure outweighs the damage to national security that might be reasonably expected from disclosure and, if the determination is affirmative, declassify the information.

§ 1203.603 Systematic review for declassification.

(a) *General.* (1) Except for foreign government information as provided in Subpart G of this part, classified information constituting permanently valuable records of the Government, as defined by 44 U.S.C. 2103, and information in the possession and control of the Administrator of General Services, pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes 20 years old. Transition to systematic reviews at 20 years shall be implemented as rapidly as practicable and shall be completed by December 1, 1988.

(2) The Administrator may extend classification beyond 20 years, but only in accordance with §§ 1203.600, 1203.601 and 1203.602 and paragraph (b) of this section. This authority may not be delegated. When classification is extended beyond 20 years, a date no more than 10 years later shall be set for declassification or for the next review. That date and specified action shall be marked on the document. Subsequent reviews for declassification shall be set at no more than 10-year intervals unless a longer interval has been authorized by the Director of the Information Security Oversight Office.

(3) A request for extension of the period between subsequent reviews for specific categories of documents or information shall be submitted to the Chairperson, NASA Information Security Program Committee, and shall include personal certification that the classified information for which the waiver is sought was systematically reviewed as required, that a definitive date for declassification could not be determined, and that results of the review established an identifiable need to retain classification for a period in excess of 20 additional years and a recommendation concerning the interval before the next required review.

(4) The Chairperson, NASA Information Security Program Committee, shall designate experienced personnel to assist the Archivist of the United States in the systematic review of 20-year old U.S. originated information and 30-year old foreign information. Such personnel shall:

(i) Provide guidance and assistance to National Archives employees in identifying and separating documents and specific categories of information within documents which are deemed to require continued classification; and

(ii) Develop reports of information or document categories so separated, with recommendations concerning continued classification.

(b) *Systematic Review Guidelines.* The Chairperson, NASA Information Security Program Committee, shall develop, in coordination with NASA organizational elements, guidelines for the systematic review for declassification of 20-year old classified information under NASA's jurisdiction. (See § 1203.700, Foreign Government Information.) The guidelines shall state specific limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection beyond 20 years is needed. These guidelines are authorized for use by the Archivist of the United States and, with the approval of the Administrator, by an agency having custody of the information covered by the guidelines. All information, except foreign government information, not identified in these guidelines as requiring review and for which a prior automatic declassification date has not been established shall be declassified automatically at the end of 20 years from the date of original classification. The guidelines shall be reviewed at least every other year and revised as necessary unless earlier review for revision is requested by the Archivist of the United States. Copies of the declassification guidelines promulgated by NASA will be provided to the Information Security Oversight Office, GSA.

(c) *Systematic Review Procedures.* (a) All security classified records 20 years old or older, whether held in storage areas under installation control or in Federal Records Centers, will be surveyed to identify those that require scheduling for future disposition. Such scheduling must be accomplished by December 1, 1980.

(2) All NASA information or material in the custody of the National Archives and Records Service that is permanently valuable and more than 20 years old is to be systematically reviewed for declassification by the Archivist of the United States with the assistance of the personnel designated for the purpose pursuant to paragraph (a)(4)(i) of this section. The Archivist shall refer to NASA that information or material which NASA has indicated requires further review. In the case of 20-year old information or material in the custody of NASA installations, such review will be accomplished by the custodians of the information or material. The installation having primary jurisdiction over the information or material received from the Archivist or in its custody, shall proceed as follows:

(i) Classified information or material over which NASA exercises exclusive or final original classification authority and which is to be declassified in accordance with the systematic review guidelines developed under paragraph (b) of this section shall be so marked.

(ii) Classified information or material over which NASA exercises exclusive or final original classification authority and which, in accordance with the systematic review guidelines developed under paragraph (b) of this section, is to be kept protected, shall be listed by category by the responsible custodian and referred to the Chairperson, NASA Information Security Program Committee. This listing shall:

(A) Identify the information or material involved.

(B) Recommend classification beyond 20 years to a specific future event scheduled to happen or a specific period of time not to exceed 10 years or, in the alternative, recommend a subsequent review date not to exceed 10 years.

(C) State the reason for the recommended continued classification.

(iii) The Administrator shall consider and determine which category of information or material shall be kept classified and the dates for automatic declassification or subsequent review. The Archivist of the United States will be notified in writing of this decision.

(d) *Declassification by the Director of the Information Security Oversight Office.* If the Director of the Information Security Oversight Office, GSA, determines that NASA information is classified in violation of Executive Order 12065, the Director may require the information to be declassified. Any such decision by the Director may be appealed through the NASA Information Security Program Committee to the National Security Council. The

information shall remain classified until the appeal is decided or until 1 year from the date of the determination by the Director of the Information Security Oversight Office, whichever comes first.

§ 1203.604 Mandatory review for declassification.

(a) *Information covered.* All classified information, except as provided below, upon request by a member of the public or a Government employee or agency to declassify and release such information under the provisions of Executive Order 12065, shall be subject to review by the originating NASA organization for possible declassification in accordance with the procedures of this section. After review, the information or any reasonable segregable portion thereof that no longer requires protection shall be declassified and released unless withholding is otherwise warranted under applicable law.

(b) *Presidential Papers.* (1) Information less than 10 years old which was originated by the President, by the White House Staff, or by committees or commissions appointed by the President, or by others acting on behalf of the President, is exempted from mandatory review for declassification.

(2) Such information 10 years old or older is subject to mandatory review for declassification in accordance with procedures developed by the Archivist of the United States which provide for consultation with NASA in matters of primary subject interest to NASA.

(c) *Submission of requests for review.* Requests for mandatory review of classified information shall be submitted in accordance with the following:

(1) Requests originating within NASA shall, in all cases, be submitted directly to the NASA installation which originated the information.

(2) For most expeditious action, requests from other Governmental agencies or from members of the public should be submitted directly to NASA installations which originated the material, or, if the originating component is not known, the requestor may submit the request to:

(i) The Chairperson, NASA Information Security Program Committee; or the head of the NASA organization most concerned with the subject matter of the material requested; or

(ii) The office designated to receive requests for records under the Freedom of Information Act pursuant to Part 1206 of this chapter.

(d) *Requirement for processing.* (1) Requests which are submitted under the Freedom of Information Act shall be processed in accordance with Part 1206 of this chapter.

(2) Other requests for declassification review and release of information shall be processed in accordance with the provisions of this section, subject to the following conditions:

(i) The request is in writing and reasonably describes the information sought with sufficient particularity to enable the installation to identify it and does not involve a large number of documents originated by numerous classifying authorities and requiring extensive coordination for accomplishment of the requested review.

(ii) The requestor shall be asked to correct a request that does not comply with paragraph (d)(2)(i) of this section, to provide additional information or to narrow the scope of the request and shall be notified that no action will be taken until the requestor complies.

(iii) If the request requires the rendering of services for which fees may not be charged under Part 1206, but may be charged under 31 U.S.C. 483a (1976), the rates prescribed in § 1206.700 shall be used, if appropriate.

(e) *Processing of Requests.* Requests that meet the requirements of paragraph (d)(2) of this section will be processed as follows:

(1) NASA installation action upon the initial request shall be completed within 60 days.

(2) Receipt of the request shall be acknowledged promptly. The NASA installation shall determine whether, under the declassification provisions of this Part 1203, the requested information may be declassified and, if so, shall make such information 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 of the reasons for denial, a notice of the right to appeal the determination to the Chairperson, NASA Information Security Program Committee, National Aeronautics and Space Administration, Washington, DC 20546, and a notice that such an appeal must be filed within 60 days in order to be considered.

(3) All appeals of denials of requests for declassification shall be acted upon and determined finally within 30 days after receipt and the requestor shall be advised that the appeal determination is final. If continued classification is required under the provisions of this Part 1203, the requestor shall be notified of the reasons thereof.

(4) The declassification and release of foreign government information that is subjected to mandatory review under this section shall be determined only in accordance with § 1203.703.

(5) When a NASA installation receives a request for declassification of information in a document which is in the custody of the installation but was classified by another NASA installation or Government agency, the installation shall refer the request to the classifying installation or Government agency, with a copy of the document containing the information requested when practicable, and shall notify the requestor of the referral. When NASA receives such a referral, it shall process the request in accordance with the requirements of this section and, if so requested, shall notify the referring agency of the determination made on the request.

(f) *Prohibition.* No NASA installation in possession of a classified document may, in response to a request for the document under this section or under Part 1206 of this chapter, refuse to confirm the existence or nonexistence of the document unless the fact of its existence or nonexistence would itself be classifiable under this Part 1203.

(g) *Declassification of Transferred Documents or Material.*—(1) *Material Officially Transferred.* In the case of classified information or material transferred by or pursuant to statute or Executive Order to NASA in conjunction with a transfer of functions (not merely for storage purposes) for NASA's use and as part of its official files or property, as distinguished from transfers merely for purposes of storage, NASA shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

(2) *Material Not Officially Transferred.* When any NASA installation has in its possession classified information or material originated by an agency which has since ceased to exist and that information has not been officially transferred to another department or agency, or when it is impossible for the possessing NASA installation to identify the originating agency, and a review of the material indicates that it should be downgraded or declassified, the possessing NASA installation shall be deemed to be the originating agency for the purpose of declassifying or downgrading such material. If it appears probable that another agency or another NASA organization may have a substantial interest in whether the classification of any particular information should be maintained, the possessing NASA

installation shall not exercise the power conferred upon it by this paragraph, until after consultation with any other agency or NASA organization having an interest in the subject matter.

(3) *Transfer for Storage or Retirement.* (i) Insofar as practicable, classified documents shall be reviewed to determine whether or not they can be downgraded or declassified prior to being forwarded to records centers or to the National Archives for storage. Any downgrading or declassification determination shall be indicated on each document by appropriate markings.

(ii) Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded or declassified by the Archivist of the United States in accordance with Executive Order 12065; the directives of the Information Security Oversight Office, GSA; and NASA guidelines.

(h) *Downgrading and Declassification Actions.*—(1) *Notification of changes in Classification or Declassification.* When classified material has been marked with specific dates or events for downgrading or declassification, it is not necessary to issue notices of such actions to any holders. However, when such actions are taken earlier than originally scheduled, or the duration of classification is shortened, the authority making such changes shall, to the extent practicable, ensure prompt notification to all addressees to whom the information or material was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor, and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify addressees to whom they have transmitted the classified information or material.

(2) *Posted Notice.* If prompt remarking of large quantities would be unduly burdensome, the custodian may attach declassification, downgrading, or upgrading notices to the storage unit in lieu of the remarking action otherwise required. Each notice shall indicate the change, the authority for the action, the date of the action, and the storage units to which it applies. Items withdrawn from such storage units shall be promptly remarked. However, when information subject to a posted downgrading or declassification notice is withdrawn from one storage unit solely for transfer to another, or a storage unit containing such information is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

(i) *Foreign Relations Series.* In order to permit the State Department editors of *Foreign Relations of the United States* to meet their mandated goal of publishing 20 years after the event, NASA shall assist these editors by facilitating access to appropriate classified materials in its custody and by expediting declassification review of items from its files selected for publication.

Subpart G—Foreign Government Information

§ 1203.700 Identification.

In order to qualify as foreign government information, information must fall into one of the two following categories:

(a) Information provided to the United States by a foreign government or international organization of governments, such as the North Atlantic Treaty Organizatiuon (NATO), where the United States has undertaken an obligation, expressed or implied, to keep the information in confidence. The information is considered to have been provided in confidence if it is marked in a manner indicating it is to be treated in confidence or if the circumstances of the delivery indicate that the information be kept in confidence.

(b) Information requiring confidentiality produced by the United States pursuant to a written, joint arragement with a foreign government or international organization of governments. A written, joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record of the joint arrangement.

§ 1203.701 Classification.

(a) Foreign government information that is classified by a foreign entity shall either retain its original classification designation or be marked with a United States classification designation that will ensure a degree of protection equivalent to that required by the entity that furnished the information. Original classification authority is not required for this purpose.

(b) Foreign government information that was not classified by a foreign entity but was provided to NASA with the expressed or implied obligation that it be held in confidence must be classified. Executive Order 12065 states a presumption of at least identifiable damage to the national security in the event of unauthorized disclosure of foreign government information. Therefore, such foreign government information shall be classified at least Confidential. However, at the time of classification, judicious consideration shall be given to the sensitivity of the subject matter and the impact of its unauthorized disclosure upon both the United States and the originating foreign government or organization of governments in order to determine the most appropriate level of classification. Levels above Confidential must be assigned by an original classification authority.

§ 1203.702 Duration of classification.

Foreign government information is exempt from the declassification and 20-year systematic review requirements of § 1203.603(b). Unless the guidelines for the systematic review of 30-year old foreign government information developed pursuant to § 1203.603(b) prescribe dates or events for declassification or for review for declassification:

(a) Foreign government information shall not be assigned a date or event for declassification unless such is specified or agreed to by the foreign entity.

(b) Foreign government information classified after December 1, 1978, shall be assigned a date for review for declassification at 30 years from the time the information was originated by the foreign entity or acquired or classified by NASA, whichever is earlier. Such information received undated shall be dated upon receipt.

§ 1203.703 Declassification.

(a) In weighing the public interest in disclosure against the need to protect foreign government information and confidential foreign sources, the need to protect such information shall be presumed to predominate.

(b) Following consultation with the Archivist of the United States and, where appropriate, with the foreign government or international organization concerned, and, with the assistance of the Department of State, NASA will issue guidelines for the systematic review of 30-year old foreign government information that will apply to foreign government information of primary concern to NASA. These guidelines are authorized for use by the Archivist of the United States and, with the approval of NASA, by an agency having custody of such information. The Chairperson, Information Security Program Committee, will initiate administrative functions necessary to effect review of these guidelines at least once every two years and submit recommendations to the Administrator based on these reviews. If, after applying the guidelines to 30-year old

foreign government information, a determination is made by the reviewer that continued classification is necessary, a date for declassification or for review no more than 10 years later shall be set. That action and date shall be marked on the document. Subsequent review dates shall be set at no more than 10-year intervals.

(c) Requests for mandatory review for declassification of foreign government information shall be processed and acted upon in accordance with the provisions of § 1203.603 except that foreign government information will be declassified only in accordance with the guidelines developed for that purpose under § 1203.702 and after consultation with other Government agencies with subject matter interest as necessary. In those cases where these guidelines cannot be applied to the foreign government information requested, the foreign originator normally should be consulted, through appropriate channels, prior to final action on the request. However, when the responsible NASA installation knows the foreign originator's view toward declassification or continued classification of the types of information requested, consultation with the foreign originator is not necessary.

(d) Requests for mandatory review for declassification of foreign government information which NASA has not received or classified shall be referred to the Government agency having a primary interest. The requestor shall be advised of the referral.

Robert A. Frosch,

Administrator.

[FR Doc. 79-18974 Filed 6-15-79; 8:45 am]

BILLING CODE 7510-01-M

FEDERAL TRADE COMMISSION

16 CFR Part 13

[Docket No. C-2964]

Prohibited Trade Practices, and Affirmative Corrective Actions; Aluminum Company of America, et al.

AGENCY: Federal Trade Commission.

ACTION: Final Order.

SUMMARY: In settlement of alleged violations of federal law prohibiting unfair acts and practices and unfair methods of competition, this consent order, among other things, requires a Pittsburgh, Pa. producer of aluminum building products and its subsidiary, Alcoa Building Products, Inc., to cease disseminating or participating in the dissemination of advertisements which contain fuel reduction, heat loss reduction, energy savings or thermal insulation representations regarding residential aluminum siding. The order also requires that the R-value for insulating material be disclosed in advertisements which merely use the term "insulated aluminum siding" for descriptive purposes.

DATES: Complaint and order issued May 11, 1979.[1]

FOR FURTHER INFORMATION CONTACT: Paul R. Peterson, Director, 4R, Cleveland Regional Office, Federal Trade Commission, 1339 Federal Office Building, 1240 East Ninth St., Cleveland, Ohio, 44199, (216) 522-4207.

SUPPLEMENTARY INFORMATION: On Friday, January 12, 1979, there was published in the **Federal Register**, 44 FR 2600, a proposed consent agreement with analysis In the Matter of Aluminum Company of America, a corporation, and Alcoa Building Products, Inc., a corporation, for the purpose of soliciting public comment. Interested parties were given sixty (60) days in which to submit comments, suggestions, or objections regarding the proposed form of order.

Comments were filed and considered by the Commission. The Commission has ordered the issuance of the complaint in the form contemplated by the agreement, made its jurisdictional findings and entered its order to cease and desist, as set forth in the proposed consent agreement, in disposition of this proceeding.

The prohibited trade practices and/or corrective actions, as codified under 16 CFR Part 13, are as follows:

Subpart-Disseminating Advertisements, Etc.: § 13.1043 Disseminating advertisements, etc.

(Sec. 6, 38 Stat. 721; (15 U.S.C. 46). Interprets or applies sec. 5, 38 Stat. 719, as amended; (15 U.S.C. 45))

Carol M. Thomas,

Secretary.

[FR Doc. 79-18921 Filed 6-15-79; 8:45 am]

BILLING CODE 6750-01-M

16 CFR Part 13

[Docket No. C-2966]

Prohibited Trade Practices, and Affirmative Corrective Actions; General Motors Corporation

AGENCY: Federal Trade Commission.

ACTION: Final Order.

SUMMARY: In settlement of alleged violations of federal law prohibiting unfair acts and practices and unfair methods of competition, this consent agreement, among other things, requires a Detroit, Mich. motor vehicle manufacturer to cease misrepresenting the manufacturing source of engine options and the availability of standard or optional equipment. The order also requires the firm to make designated disclosures regarding the manufacturing source, ordering code, and availability of each engine option offered for the model years 1979 through 1981; notify dealers promptly of engine option substitutions; and provide them with the replacement parts and maintenance information necessary to service such equipment. Additionally, the company is prohibited from using any wholesale order system which could prevent dealers from designating specific options requested by purchasers.

DATES: Complaint and order issued May 18, 1979.[1]

FOR FURTHER INFORMATION CONTACT: Paul R. Peterson, Director, 4R, Cleveland Regional Office, Federal Trade Commission, 1339 Federal Office Bldg., 1240 East Ninth St., Cleveland, Ohio. 44199. (216) 522-4207.

SUPPLEMENTARY INFORMATION: On Friday, January 26, 1979, there was published in the **Federal Register**, 44 FR 5457, a proposed consent agreement with analysis In the Matter of General Motors Corporation, a corporation, for the purpose of soliciting public comment. Interested parties were given sixty (60) days in which to submit comments, suggestions, or objections regarding the proposed form of order.

Comments were filed and considered by the Commission. The Commission has ordered the issuance of the complaint in the form contemplated by the agreement, made its jurisdictional findings and entered its order to cease and desist, as set forth in the proposed consent agreement, in disposition of this proceeding.

The prohibited trade practices and/or corrective actions, as codified under 16 CFR Part 13, are as follows:

Subpart-Advertising Falsely or Misleadingly: § 13.10 Advertising falsely or misleadingly; 13.10-1 Availability of merchandise and/or facilities; § 13.90 History of product or offering; § 13.160 Promotional sales plans; § 13.205 Scientific or other relevant facts; § 13.235 Source or origin; 13.235-35 History. Subpart-Corrective Actions and/or Requirements: § 13.533 Corrective actions and/or requirements; 13.533-20 Disclosures. Subpart-Misrepresenting Oneself and Goods—

[1] Copies of the Complaint, and the Decision and Order filed with the original document.

[1] Copies of the Complaint, and the Decision and Order filed with the original document.