AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

§ 1201.401 Special document depositories.

NASA provides the National Technical Information Service (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161, with copies of NASA and/or NASA-sponsored unclassified unlimited documents to provide availability to the public. These documents may be reproduced by NTIS and sold at prices established by NTIS. NASA also uses the regional depository libraries established through the Federal Depository Library Program by chapter 19 of title 44 of the U.S. Code under the Government Printing Office (GPO) to make its technical documents and bibliographic tools available to the general public. These depository libraries are responsible for permanent retention of material, interlibrary loan, and reference services.

§ 1201.402 NASA Industrial Applications Centers.

(a) As part of its Technology Utilization Program—a program designed to transfer new aerospace knowledge and innovative technology to nonaerospace sectors of the economy—NASA operates a network of Industrial Applications Centers. These centers serve U.S. industrial clients on a fee paying basis by providing access to literally millions of scientific and technical documents published by NASA and by other research and development organizations. Using computers, the NASA Industrial Applications Centers conduct retrospective and current awareness searches of available literature in accordance with client interests, and assist in the interpretation and adaption of retrieved information to specified needs. Such services may be obtained by contacting one of the following:

(1) Aerospace Research Applications Center (ARAC), Indianapolis Center for Advanced Research, 611 N. Capital Avenue, Indianapolis, IN 46204.

(2) Southern Technology Applications Center, Progress Center, Box 24, 1 Progress Boulevard, Alachua, FL 32615.

(3) NASA/UK Technology Applications Program, University of Kentucky, 10 Kinkead Hall, Lexington, KY 40506–0057.

(4) NASA Industrial Applications Center, 823 William Pitt Union, University of Pittsburgh, Pittsburgh, PA 15260.

(5) New England Research Application Center (NERAC), One Technology Drive, Tolland, CT 06084.

(6) North Carolina Science and Technology Research Center, P.O. Box 12235, Research Triangle Park, NC 27709.

(7) Technology Application Center (TAC), University of New Mexico, Albuquerque, NM 87131.

(8) Kerr Industrial Applications Center, Southeastern Oklahoma State University, Station A, Box 2584, Durant, OK 74701.

(9) NASA Industrial Applications Center, Research Annex, Room 200, University of Southern California, 3716 South Hope Street, Los Angeles, CA 90007.

(10) NASA/SU Industrial Applications Center, Southern University, Department of Computer Science, Baton Rouge, LA 70813–2065.

(b) To obtain access to NASA-developed computer software, contact: Computer Software Management and Information Center (COSMIC), University of Georgia, Athens, GA 30602.

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.
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 Limitations.
1203.411 Restrictions.
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 Authorization.
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.

Subpart H—Delegation of Authority To Make Determinations in Original Classification Matters

1203.800 Delegations.
1203.801 Redelegation.
1203.802 Reporting.

Subpart I—NASA Information Security Program Committee

1203.900 Establishment.
1203.901 Responsibilities.
1203.902 Membership.
1203.903 Ad hoc committees.
1203.904 Meetings.

AUTHORITY: 42 U.S.C. 2451 *et seq.* and E.O. 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333.

SOURCE: 44 FR 34913, June 18, 1979, unless otherwise noted.

Subpart A—Scope

§ 1203.100 Legal basis.

(a) *Executive Order 12356 (hereinafter referred to as ''the Order'')*. 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 the ''the Order'' (47 FR 14874) and the Information Security Oversight Office Directive No. 1, June 25, 1982;

(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.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5889, Feb. 9, 1983]

§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) In recognition of the essential requirement for an informed public concerning the activities of its Government, as well as the need to protect certain national security information from unauthorized disclosure, ''the Order'' was promulgated. It designates the National Aeronautics and Space Administration 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 limitations and restrictions as discussed in §§1203.410 and 1203.411.

(c) ''The Order'' 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 damage to the national security.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5889, Feb. 9, 1983]

§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 ''the Order'' 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 30-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 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 responsibilities listed in paragraphs (e)(1), (2), and (3) of this section may be reassigned.

(f) The Senior Security Specialist, NASA Security Office, 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 Chief, Information and Physical Security Branch, NASA Security Office, is responsible for establishing procedures for the safeguarding of classified information of material (e.g., accountability, control, access, storage, transmission, and marking) and for ensuring that such procedures are systematically reviewed; and those which are duplicative or unnecessary are eliminated.

[44 FR 34913, June 18, 1979, as amended at 45 FR 3888, Jan. 21, 1980; 48 FR 5890, Feb. 9, 1983; 53 FR 41318, Oct. 21, 1988]

§1203.203 Degree of protection.

(a) *General.* Upon determination that information or material must be classified, the degree of protection commensurate with the sensitivity of the information must be determined. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days.

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

(1) *Top Secret.* Top Secret is the designation applied to information or material the unauthorized 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 unauthorized 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 developments relating to national security.

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

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983]

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 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 under ''the Order.''

(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, and would result in damage to such a system, subsystem or component.

(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 any U.S. space mission, that might result in 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.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983]

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

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

[48 FR 5890, Feb. 9, 1983]

§ 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 Limitations.

(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 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 or to prevent or delay the public release of such information.

(f) Information may be classified or reclassified after receipt of a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of ''the Order'' if such classification meets the requirements of ''the Order'' and is accomplished personally on a document-by-document basis by an official with original Top Secret classification authority.

(g) The Administrator, the Chairperson, NASA Information Security Program Committee, or an official with original Top Secret classification authority may reclassify information previously declassified and disclosed if it is determined in writing that (1) The information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office, GSA.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5890, Feb. 9, 1983]

§1203.411 Restrictions.

(a) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this section, the Department of Defense shall be considered one agency.

(b) Classified information shall not be disseminated outside the Executive Branch except under conditions that ensure the information will be given

protection equivalent to that afforded within the Executive Branch.

[48 FR 5890, Feb. 9, 1983]

§ 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 specified classification in terms of a period of time or future event. Whenever a specific time or future event for declassification cannot be predetermined, the following notation will be used: DECLASSIFY ON: Originating Agency's Determination Required or ''OADR.''

(4) Indicate specifically that the designations, time limits, markings and other requirements of ''the Order'' 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.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5891, Feb. 9, 1983]

Subpart E—Derivative Classification

§ 1203.500 Use of derivative classification.

The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form information that is already classified, and of those who apply markings in accordance with instructions from an authorized original classifier or in accordance with an authorized classification guide. If a person who applied derivative classification markings believes that the paraphrasing, restating, or summarizing of classified information has changed the level of or removed the basis for classification, that person must consult for a determination with an appropriate official of the originating agency or office of origin who has the authority to upgrade, downgrade, or declassify the information.

[48 FR 5891, Feb. 9, 1983]

§ 1203.501 Applying derivative classification markings.

Persons who apply derivative classification markings shall:

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

[44 FR 34913, June 18, 1979, as amended at 48 FR 5891, Feb. 9, 1983]

Subpart F—Declassification and Downgrading

§ 1203.600 Policy.

Information shall be declassified or downgraded as soon as national security considerations permit. NASA reviews of classified information shall be coordinated with other agencies that have a direct interest in the subject matter. Information that continues to

meet the classification requirements prescribed by §1203.400 despite the passage of time will continue to be protected in accordance with ''the Order.''

[48 FR 5891, Feb. 9, 1983]

§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 Authorization.

Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position, the originator's successor, a supervisory official of either, or officials delegated such authority in writing by the Administrator or the Chairperson, NASA Information Security Program Committee.

[48 FR 5891, Feb. 9, 1983]

§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 Administration pursuant to 44 U.S.C. 2107 or 2107 note, shall be reviewed for declassification as it becomes 30 years old.

(2) Systematic review for declassification of classified cryptologic information will be coordinated through the National Security Agency.

(3) Systematic review for declassification of classified information pertaining to intelligence activities (including special activities) or intelligence sources or methods will be coordinated through the Central Intelligence Agency.

(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 30-year old U.S. originated information and 30-year old foreign information. Such personnel shall:

(i) Provide guidance and assistance to National Archives and Records Service 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 30-year old classified information under NASA's jurisdiction. (See subpart G of this part, 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 30 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, cryptologic information, and information pertaining to intelligence sources or methods, 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 30 years from the date of original classification. These guidelines shall be reviewed at least every 5 years and revised as necessary unless an 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.* (1) All security classified records 30 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.

(2) All NASA information or material in the custody of the National Archives and Records Service that is permanently valuable and more than 30 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 30-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 jurisdication 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 30 years to a specific event scheduled to happen or a specific period of time or, the alternative, recommend: DECLASSIFY ON: Originating Agency's Determination Required or ''OADR.''

(iii) The Administrator shall consider and determine which category shall be kept classified and the dates or event for declassification. Whenever a specific time or future event for declassification cannot be predetermined, the following notation will be applied: DECLASSIFY ON: Originating Agency's Determination Required or ''OADR.'' 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, GSA.* If the Director of the Information Security Oversight Office, GSA, determines that NASA information is classified in violation of ''the Order,'' 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 pending a prompt decision on the appeal.

[48 FR 5891, Feb. 9, 1983]

§ 1203.604 Mandatory review for declassification.

(a) *Information covered.* All information classified under ''the Order'' or predecessor orders, except as provided at § 1203.604(b) shall be subject to a review for declassification by the originating agency, if:

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

(2) The request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort. 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 originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of § 1203.604(a).

(2) The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services Administration or the Archivist pursuant to sections 2107, 2107 note, or 2203 of Title 44, U.S. Code. Review procedures developed by the Archivist shall 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 specifically citing 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.

(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 any request for declassification of information in documents in its custody that was classified by another NASA installation or Government agency, it shall refer copies of the request and the requested documents to the originating installation or agency for processing, and may, after consultation with the originating installation or agency, inform the requester of the referral. In cases in which the originating NASA installation determines in writing that a response under §1203.604(f) is indicated, such cases will be promptly forwarded to the Chairperson, NASA Information Security Program Committee, for final resolution and appropriate response.

(f) *Neutral response.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of ''the Order,'' NASA shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under ''the Order.''

(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 ''the Order,'' 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.

(ii)[Reserved]

[44 FR 34913, June 18, 1979, as amended at 45 FR 3888, Jan. 21, 1980; 48 FR 5892, Feb. 9, 1983; 53 FR 41318, Oct. 21, 1988]

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 arrangement 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. ''The Order'' states that unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security. 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.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5892, Feb. 9, 1983]

§1203.702 Duration of classification.

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:

(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 annotated: DECLASSIFY ON: Originating Agency's Determination Required or ''OADR.''

[48 FR 5893, Feb. 9, 1983]

§1203.703 Declassification.

(a) Information classified in accordance with §1203.400 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

(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, NASA Information Security Program Committee, will initiate administrative functions necessary to effect review of these guidelines at least once every 5 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 classification is necessary, a date for declassification or DECLASSIFY ON: Originating Agency's Determination Required or ''OADR'' shall be shown on the face of the document.

(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.

[44 FR 34913, June 18, 1979, as amended at 48 FR 5893, Feb. 9, 1983]

Subpart H—Delegation of Authority To Make Determinations in Original Classification Matters

SOURCE: 62 FR 54380, Oct. 20, 1997, unless otherwise noted.

§ 1203.800 Delegations.

(a) The NASA officials listed in paragraph (b) (1) and (2) of this section are authorized to make, modify, or eliminate security classification assignments to information under their jurisdiction for which NASA has original classification authority. Such actions shall be in accordance with currently applicable criteria, guidelines, laws, and regulations, and they shall be subject to any contrary determination that has been made by the Senior Agency Official for Classified National Security Information, or by any other NASA official authorized to make such a determination. The Director, Security Management Office, is designated to act as the Senior Agency Official for Classified National Security Information. The NASA officials listed in paragraph (b)(3) of the section are authorized to declassify top Secret security classification assignments over 25 years old to information under their jurisdiction for which NASA has original classification authority. The NASA officials listed in paragraphs (b)(4) of this section are authorized to declassify Secret and Confidential security classification assignments to information under their jurisdiction for which NASA has original classification authority.

(b) *Designated officials*—(1) *TOP SECRET Classification Authority*. (i) Administrator.

(ii) Deputy Administrator.

(iii) Associate Deputy Administrator.

(iv) Associate Deputy Administrator (Technical).

(v) Senior Agency Official for Classified National Security Information.

(2) *SECRET and CONFIDENTIAL Classification Authority*. Officials listed in paragraph (b)(1) of this section.

(3) *Declassification Authority, Top Secret Assignments over 25 years Old*. (i) Agency Security Program Manager, NASA Headquarters.

(ii) Such other officials as may be delegated declassification authority, in

writing, by the Senior Agency Official for Classified National Security Information.

(4) *Declassification Authority, Secret and Confidential.* (i) Security Administrative Team Leader, Headquarters NASA.

(ii) Such other officials as may be delegated declassification authority, in writing, by the Senior Agency Official for Classified National Security Information.

(c) Written requests for original classification authority or declassification authority shall be forwarded to the Senior Agency Official for Classified National Security Information, with appropriate justification appended thereto.

(d) The Senior Agency Official for Classified National Security Information shall maintain a list of all delegations of original classification of declassification authority by name or title of the position held.

(e) The Senior Agency Official for Classified National Security Information shall conduct a periodic review of delegation lists to ensure that the officials so designated have demonstrated a continuing need to exercise such authority.

(f) Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide.

§1203.801 Redelegation.

Redelegation of TOP SECRET, SECRET, or CONFIDENTIAL original classification authority or declassification authority is not authorized.

§1203.802 Reporting.

The officials to whom original classification authority has been delegated under this section shall ensure that feedback is provided to the Senior Agency Official for National Security Information. The Senior Agency Official for National Security Information shall keep the Administrator currently informed of all significant actions, problems, or other matters of substance related to the exercise of the authority delegated hereunder.

Subpart I—NASA Information Security Program Committee

SOURCE: 54 FR 6881, Feb. 15, 1989, unless otherwise noted.

§1203.900 Establishment.

Pursuant to Executive Order 12356, ''National Security Information,'' and the National Aeronautics and Space Act of 1958, as amended, there is established a NASA Information Security Program Committee (hereinafter referred to as the Committee) as part of the permanent administrative structure of NASA. The Director, NASA Security Office, is designated to act as the Chairperson of the Committee. The Senior Security Specialist, Classification Management and Physical Security Section, NASA Security Office, is designated to act as the Committee Executive Secretary.

§1203.901 Responsibilities.

(a) The Chairperson reports to the Administrator concerning the management and direction of the NASA Information Security Program as provided for in subpart B of this part. In this connection, the Chairperson is supported and advised by the Committee.

(b) The Committee shall act on all appeals from denials of declassification requests and on all suggestions and complaints with respect to administration of the NASA Information Security Program as provided for in subpart B of this part.

(c) The Executive Secretary of the Committee shall maintain all records produced by the Committee, its subcommittees, and its ad hoc panels.

(d) The NASA Security Office, NASA Headquarters, will provide staff assistance, and investigative and support services for the Committee.

§1203.902 Membership.

The Committee will consist of the Chairperson and Executive Secretary. In addition, each of the following NASA officials will nominate one person to Committee membership:

(a) Associate Administrators for:

(1) Aeronautics and Space Technology.

(2) Space Science and Applications.

(3) Space Flight.
(4) Space Station.
(5) Space Operations.
(6) Management.
(7) External Relations.
(8) Safety, Reliability, Maintainability and Quality Assurance.
(b) Associate Deputy Administrator.
(c) General Counsel.
Other members may be designated upon specific request of the Chairperson.

§ 1203.903 Ad hoc committees.

The Chairperson is authorized to establish such ad hoc panels or subcommittees as may be necessary in the conduct of the Committee's work.

§ 1203.904 Meetings.

(a) Meetings will be held at the call of the Chairperson.
(b) Records produced by the Committee and the minutes of each meeting will be maintained by the Executive Secretary.

PART 1203a—NASA SECURITY AREAS

Sec.
1203a.100 Purpose and scope.
1203a.101 Definitions.
1203a.102 Establishment, maintenance, and revocation of security areas.
1203a.103 Access to security areas.
1203a.104 Violation of security areas.
1203a.105 Implementation by field and component installations.

AUTHORITY: 18 U.S.C. 799.

SOURCE: 38 FR 8056, Mar. 28, 1973, unless otherwise noted.

§ 1203a.100 Purpose and scope.

(a) To insure the uninterrupted and successful accomplishment of the NASA mission, certain designated security areas may be established and maintained by NASA installations and component installations in order to provide appropriate and adequate protection for facilities, property, or classified information and material in the possession or custody of NASA or NASA contractors located at NASA installations and component installations.
(b) This part 1203a sets forth:
(1) The designation and maintenance of security areas,
(2) The responsibilities and procedures in connection therewith, and
(3) The penalties that may be enforced through court actions against unauthorized persons entering security areas.

§ 1203a.101 Definitions.

For the purpose of this part, the following definitions apply:
(a) *Security area.* A physically defined area, established for the protection or security of facilities, property, or classfied information and material in the possession or custody of NASA or a NASA contractor located at a NASA installation or component installation, entry to which is subject to security measures, procedures, or controls. Security areas which may be established are:
(1) *Restricted area.* An area wherein security measures are applied primarily for the safeguarding or the administrative control of property or to protect operations and functions which are vital or essential to the accomplishment of the mission assigned to a NASA installation or component installation.
(2) *Limited area.* An area wherein security measures are applied primarily for the safeguarding of classified information and material or unclassified property warranting special protection and in which the uncontrolled movement of visitors would permit access to such classified information and material or property, but within which area such access may be prevented by appropriate visitor escort and other internal restrictions and controls.
(3) *Closed area.* An area wherein security measures are applied primarily for the purpose of safeguarding classified information and material; entry to the area being equivalent, for all practical purposes, to access to such classified information and material.
(b) *Temporary security area.* A designated interim security area, the need for which will not exceed 30 days from date of establishment. A temporary security area may also be established on an interim basis, pending approval of its establishment as a permanent security area.