

§ 1203.404

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 Adminis-

14 CFR Ch. V (1-1-05 Edition)

tration, 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 originates 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