

§ 1203.304

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 progress 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

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

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