§ 2400.3 Applicability.

This Regulation governs the Office of Science and Technology Policy Information Security Program. In accordance with the provisions of Executive Order 12356 and Directive No. 1 it establishes, for uniform application throughout the Office of Science and Technology Policy, the policies and procedures for the security classification, downgrading, declassification and safeguarding of information that is owned by, produced for or by, or under the control of the office of Science and Technology Policy.

§ 2400.4 Atomic Energy Material.

Nothing in this Regulation supersedes any requirement made by or under the Atomic Energy act of 1954, as amended. ''Restricted Data'' and information designated as ''Formerly Restricted Data'' shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued pursuant thereto by the Department of Energy.

Subpart B—Original Classification

§ 2400.5 Basic policy.

Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, as implemented by Directive No. 1 and this Regulation, provides the only basis for classifying information. The policy of the Office of Science and Technology Policy is to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security. Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security.

§ 2400.6 Classification levels.

(a) National security information (hereinafter ''classified information'') shall be classified at one of the following three levels:

(1) ''Top Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) ''Secret'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) ''Confidential'' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information. Markings other than ''Top Secret,'' ''Secret,'' and ''Confidential,'' such as ''For Official Use Only,'' shall not be used to identify national security information. In addition, no other term or phrase shall be used in conjunction with one of the three authorized classification levels, such as ''Secret Sensitive'' or ''Agency Confidential.'' The terms ''Top Secret'', ''Secret'', and ''Confidential'' should not be used to identify nonclassified executive branch information.

(c) Unnecessary classification, and classification at a level higher than is necessary shall be scrupulously avoided.

(d) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified ''Confidential'' pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification the originator of the information shall safeguard it at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days. Upon the determination of a need for classification and/or the proper classification level, the information that is classified shall be marked as provided in § 2400.12 of this part.

§ 2400.7 Original classification authority.

(a) Authority for original classification of information as Top Secret shall be exercised within OSTP only by the

Director and by such principal subordinate officials having frequent need to exercise such authority as the Director shall designate in writing.

(b) The authority to classify information originally as Secret shall be exercised within OSTP only by the Director, other officials delegated in writing to have original Top Secret classification authority, and any other officials delegated in writing to have original Secret classification authority.

(c) The authority to classify information originally as Confidential shall be exercised within OSTP only by officials with original Top Secret or Secret classification authority and any officials delegated in writing to have original Confidential classification authority.

§ 2400.8 Limitations on delegation of original classification authority.

(a) The Director, OSTP is the only official authorized to delegate original classification authority.

(b) Delegations of original classification authority shall be held to an absolute minimum.

(c) Delegations of original classification authority shall be limited to the level of classification required.

(d) Original classification authority shall not be delegated to OSTP personnel who only quote, restate, extract or paraphrase, or summarize classified information or who only apply classification markings derived from source material or as directed by a classification guide.

(e) The Executive Director, OSTP, shall maintain a current listing of persons or positions receiving any delegation of original classification authority. If possible, this listing shall be unclassified.

(f) Original classification authority may not be redelegated.

(g) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of OSTP that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with these Regulations as provided in § 2400.6(d) of this part. The information shall be transmitted promptly as provided in these Regulations to the official in OSTP who has appropriate subject matter interest and classification authority with respect to this information. That official shall decide within thirty (30) days whether to classify this information. If the information is not within OSTP's area of classification responsibility, OSTP shall promptly transmit the information to the responsible agency. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

§ 2400.9 Classification requirements.

(a) Information may be classified only if it concerns one or more of the categories cited in Executive Order 12356, as subcategorized below, *and* an official having original classification authority determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(1) Military plans, weapons or operations;

(2) The vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities (including special activities), or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) United States Government programs for safe-guarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information which are related to national security and that require protection against unauthorized disclosure as determined by the Director, Office of Science and Technology Policy. Each such determination shall be reported promptly to