

Office of the Vice President of the U.S.

§ 2800.6

be stored in a safe at the close of business, destroyed as classified waste when no longer serviceable, etc.

(9) *Inventories.* The Staff Security Office will conduct inventories of all TOP SECRET material charged to the Office of the Vice President at least annually to determine the adequacy of control procedures and insure accountability.

(i) *Loss or compromise.* Any person who has knowledge of loss of possible compromise of classified information shall promptly report the circumstances to the Staff Security Office for appropriate action in accordance with ISOO Directive No. 1, paragraph IV, H.

(j) *Penalties.* Any individual breach of security may warrant penalties up to and including the separation of the individual from his employment or criminal prosecution.

(k) *Special access.* Special access authority is required for release of Sensitive Compartmented Intelligence Information. The names of personnel cleared for access to this category of information are on file in the Staff Security Office.

§ 2800.5 Policies.

(a) *Basic policy.* Except as provided in the Atomic Energy Act of 1943, as amended, Executive Order 12065, as implemented by ISOO Directive No. 1, provides the only basis for classifying information. It is the policy of this office to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

(b) *Duration of classification.* Classification shall not be continued longer than necessary for the protection of national security. Each decision to classify requires a simultaneous determination of the duration such classification must remain in effect. For further guidance, refer to sections 1-401 and 1-402, E.O. 12065.

(c) *Declassification.* Declassification of information shall be given emphasis comparable to that accorded to classification. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the

passage of time or upon the occurrence of a declassification event. For further guidance, refer to sections 3-102, 3-103 and 3-104 of E.O. 12065.

(d) *Systematic review for declassification.* Systematic review for declassification will be in accordance with sections 3-204, 3-401 and 3-503 of E.O. 12065.

(e) *Mandatory review requests.* Requests from a member of the public, a government employee, or an agency, to declassify and release information will be acted upon within 60 days provided the request reasonably identifies the information. After review, the information or any reasonably segregable portion thereof that no longer requires protection, shall be declassified and released, except as provided in section 3-503, E.O. 12065, unless withholding is otherwise warranted under applicable law.

(f) *Classification guides.* The Chief Counsel, National Security Council, has determined that, in view of the limited amount of material originally classified by this office, the preparation and publication of classification guides is not required.

(g) *Access to Classified Information by historical researchers and former Presidential appointees.* Access may be granted under the provisions of section 4-3 of E.O. 12065; however, access is permissive and not mandatory.

§ 2800.6 Delegation of classification and declassification authority.

Pursuant to the provisions of sections 1-201 and 3-103 of E.O. 12065 of June 28, 1978, the following officials within the Office of the Vice President, are designated to originally classify and declassify information as "SECRET" and/or "CONFIDENTIAL":

(a) Chief of Staff to the Vice President.

(b) Counsel to the Vice President.

(c) Executive Assistant to the Vice President.

(d) Assistant to the Vice President for National Security Affairs.

(e) Assistant to the Vice President for Issues Development and Domestic Policy.

(f) Additionally, the following individuals are designated to declassify "SECRET" and/or "CONFIDENTIAL"