that access is essential to the accomplishment of official Government duties or contractual obligations.

(b) *Determination of Trustworthiness.* A person is eligible for access to classified information only after a showing of trustworthiness as determined by the President's Personal Representative for Micronesian Status Negotiations based upon appropriate investigations in accordance with applicable standards and criteria.

§ 2700.42 Responsibility for safeguarding classified information.

(a) *General Policy.* The specific responsibility for the maintenance of the security of classified information rest with each person having knowledge or physical custody therof, no matter how obtained. The ultimate responsibility for safeguarding classified information rests on each supervisor to the same degree that supervisor is charged with functional responsibility.

(b) *Security and Top Secret Control Officers.* The Director, OMSN, and the Status Liaison Officer, Saipan, are assigned specific security responsibilities as Security Officer and Top Secret Control Officer.

(c) *Handling.* All documents bearing the terms ''Top Secret,'' ''Secret'' and ''Confidential'' shall be delivered to the Top Secret Control Officer or his designee immediately upon receipt. All potential recipients of such documents shall be advised of the names of such designees and updated information as necessary. In the event that the Top Secret Control Officer or his designees are not available to receive such documents, they shall be turned over to the office supervisor and secured, unopened, in a designated combination safe located in OMSN or SLNO, as appropriate until the Top Secret Control Officer is available. All materials not immediately deliverable to the Top Secret Control Officer shall be delivered at the earliest opportunity. Under no circumstances shall classified material that cannot be delivered to the Top Secret Control Officer be stored other than in the designated safe.

(d) *Storage.* All classified documents shall be stored in the designated combination safe or safes located in OMSN or SLNO as appropriate. The combination shall be changed as required by ISOO Directive No. 1, section IV F (5)(a). The combinations shall be known only to the Security Officer and his designees with the appropriate security clearance.

(e) *Security Education Program.* The Security Officer shall establish a program of briefings to familiarize personnel with the provisions of E.O. 12065 and implementing directives. Such briefings shall be held once per year, or more frequently. Before any new or newly assigned employee enters on duty, he shall be given instruction in sufficient detail in security procedures and practices to inform him of his responsibilities arising from his access to classified data.

(f) *Access by Historical Researchers and Former Presidential Appointees.* In keeping with provisions 4–301 and 4–302 of E.O. 12065, the President's Personal Representative for Micronesian Status Negotiations shall designate appropriate officials to determine, prior to granting access to classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

§ 2700.43 Reproduction controls.

OMSN and SLNO shall maintain records to show the number and distribution of all OMSN originated classified documents. Reproduction of classified material shall take place only in accordance with section 4–4 of E.O. 12065 and any limitations imposed by the originator. Should copies be made, they are subject to the same controls as the original document. Records showing the number of distribution of copies shall be maintained by the Office Supervisor and the log stored with the original documents. These measures shall not restrict reproduction for the purposes of mandatory review.

§ 2700.44 Administrative sanctions.

Officers and employees of the United States Government assigned to OMSN shall be subject to appropriate administrative sanctions if they knowingly and willingly commit a violation under section 5–5 of E.O. 12065. These sanctions may include reprimand, suspension without pay, removal, termination

of classification authority, or other sanction in accordance with applicable law or the applicable regulations of the agency from which they are assigned to OMSN.

Subpart F—Implementation and Review

§ 2700.51 Information Security Oversight Committee.

The OMSN Information Security Oversight Committee shall be chaired by the Security Officer, OMSN. The Committee shall be responsible for acting on all suggestions and complaints concerning the administration of the OMSN information security program. The chairperson shall also be responsible for conducting an active oversight program to ensure effective implementation of E.O. 12065.

§ 2700.52 Classified Review Committee.

The OMSN Classification Review Committee shall be chaired by the President's Personal Representative for Micronesian Status Negotiations. The Committee shall decide appeals from denials of declassification requests submitted pursuant to section 3–5 of E.O. 12065. The Committee shall consist of the President's Personal Representative, Department of Defense/Legal Advisor and Political/Economic Advisor.