APPENDIX B

DEFINITIONS

1. **Access. The** ability and opportunity to obtain knowledge of classified information.

2. **Acknowledged Special Access Program.** A SAP whose existence is known, to include association with another classified program which is publicly acknowledged.

3. Agency. An organization specified as such in E.O. 12958, as amended by E.O. 12972. Within the Department of Defense, this term includes the Department of Defense and the Departments of the Army, Navy, and Air Force.

4. **Applicable Associated Markings.** Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "classified by" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

5. **Automated Information System.** An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

6. Automatic declassification. The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under E.O. 12958.

7. **Carve-Out.** A classified contract for which the Defense Investigative Service has been relieved of inspection responsibility in whole or in part.

8. **Classification. The** actor process by which information is determined to be classified information.

9. **Classification Guidance.** Any instruction or source that prescribes the classification of specific information.

10. **Classification Guide.** A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

11. **Classified National Security Information.** (Or "Classified Information"). Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

12. Classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

13. **Code Word.** A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher.

14. **Collateral Information.** Information identified as National Security Information under the provisions of E.O. 12958 but which is not subject to enhanced security protection required for SAP Information.

15. **Communications Security (COMSEC). The** protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

16. **Compromise.** An unauthorized disclosure of classified information.

17. Confidential Source. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

18. Continental United States (CONUS). United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

19. **Controlled Cryptographic Item (CCI).** A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified but controlled.

(Equipments and components so designated bear the designator "Controlled Cryptographic Item" or 'CCL")

20. Critical **Nuclear Weapon Design Information (CNWDI).** That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fissionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test, or replace.

21. **Cryptanalysts. The** analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system of key employed in the encryption.

22. **Cryptography. The** branch of cryptology which treats the principles, means, and methods of designing and using cryptosystems.

23. **Cryptology. The** branch of knowledge which treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC).

24. Damage **to the National Security. Harm** to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

25. **Declassification. The** authorized change in the status of information from classified information to unclassified information.

26. **Declassification Authority.** a. The official who authorized the original classification, if that official is still serving in the same position; b. the originator's current successor in function; c. a supervisory official of either; or d.officials delegated declassification authority in writing by the agency head or the senior agency official.

27. **Declassification Guide.** Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

28. **Derivative Classification. The** process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

29. **Document. Any** physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

30. **DoD Component. The** Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense Agencies.

31. Downgrading. A determination that information classified at a specified level shall be classified at a lower level.

32. Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

33. **File series.** Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

34. **Foreign Government Information.** a. Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; b. information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or c. information received and treated as "Foreign Government Information" under the terms of a predecessor order to E.O. 12958.

35. **Formerly Restricted Data.** Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

36. **Information.** Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United

States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

37. Information **Security. The** system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

38. **Infraction.** Any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that does not comprise a "violation," as defined in paragraph 69 below.

39. **Integrity. The** state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

40. **Intelligence Activity.** An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333.

41. **Mandatory Declassification Review.** Review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of E.O. 12958.

42. **Material.** Any product or substance on or in which information is embodied.

43. Multiple **Sources.** Two or more source documents, classification guides, or a combination of both.

44. **National security. The** national defense or foreign relations of the United States.

45. **Need-to-know.** A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

46. **Network.** A system of two or more computers that can exchange data or information.

47. **Nickname.** A nickname is a combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

48. **Original Classification.** An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

49. **Original Classification Authority.** An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

50. **Permanent Historical Value. Those** records that have been identified in an agency records schedule as being permanently valuable.

51. **Prospective Special Access Program (P-SAP).** A DoD program or activity for which enhanced security measures have been proposed and approved to facilitate security protections prior to establishing the effort as a DoD SAP.

52. **Protective Security Service.** A transportation protective Service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (MTMC) to transport SECRET shipments. The carrier must provide continuous attendance and surveillance of the shipment by qualified carrier representatives and maintain a signature and tally record. In the case of air movement, however, observation of the shipment is not required during the period it is stored in the carrier's aircraft in connection with flight, provided the shipment is loaded into a compartment that is not accessible to an unauthorized person aboard. Conversely, if the shipment is loaded into a compartment of the aircraft that is accessible to an unauthorized person aboard, the shipment must remain under the constant surveillance of a cleared escort or qualified carrier representative.

53. **Regrade.** To raise or lower the classification assigned to an item of information.

54. **Restricted Data.** All data concerning a. design, manufacture or utilization of atomic weapons; b. the production of special nuclear material; or c. the use of special nuclear material in the production of **energy,** but shall not include data declassified or removed from the Restricted Data category under Section 142 of the Atomic Energy Act of 1954, as amended.

55. Safeguarding. Measures and controls that are prescribed to protect classified information.

56. **Security Clearance.** A determination that a person is eligible under the standards of DoD 5200.2-R for access to classified information.

57. **Security In-Depth:** A determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to use of perimeter fences,

employee and visitor access controls, use of an Intrusion Detection System, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

58. Self-Inspection. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under E.O. 12958 and its implementing directives.

59. **Senior Agency Official.** An official appointed by the Secretary of Defense, Secretary of the Army, Secretary of the Navy, or Secretary of the Air Force under the provisions of Section 5.6(c) of E.O. 12958.

60. **Senior Official.** An official appointed by the head of a DoD Component to be responsible for direction and administration of the Information Security Program. (Note: In the Departments of Defense, Army, Navy, and Air Force, this official will also be the "Senior Agency Official" as defined above.

61. **Sensitive Compartmented Information.** Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence.

62. **Special Access Program (SAP).** Any DoD program or activity (as authorized in E. O. 12958), employing enhanced security measures (e.g. safeguarding, access requirements, etc.) exceeding those normally required for collateral information at the same level of classification shall be established, approved, and managed as a DoD SAP.

63. **Special Activity.** An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

64. Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code, and is exempted from the automatic declassification provisions of section 3 of Chapter 4 of this Regulation.

65. **Telecommunications. The** preparation, transmission, or communication of information by electronic means.

66. Unacknowledged Special Access Program. A SAP, the existence of which is not acknowledged, affirmed, or made known to any person not authorized for access.

67. Unauthorized disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

68. Upgrade. To raise the classification of an item of information from one level to a higher one.

69. Violation. a.) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; b. any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directives; or c.) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E.O. 12958.

70. **Waived Special Access Program.** A SAP for which the Secretary of Defense has waived applicable reporting requirements of Section 119 of title 10, U. S. C., is identified as a "Waived SAP" and therefore has more restrictive reporting and access controls.