COMSEC Briefing and Acknowledgment Form

You have been selected to perform duties which will require access to sensitive COMSEC information. It is, therefore, essential that you are made fully aware of certain facts relative to the protection of this information before access is granted. This briefing will provide you with a description of the types of COMSEC information you may have access to. The reasons why special safeguards are necessary for protecting this information, the directives and rules which prescribe those safeguards, and the penalties which you will incur for willful disclosure of this information to unauthorized persons.

COMSEC equipment and keying materiel are especially sensitive because they are used to protect other sensitive information against unauthorized access during the process of communicating that information from one point to another. Any particular piece of COMSEC equipment, keying materiel, or other cryptographic materiel may be the critical element, which protects large amounts of sensitive information from interception, analysis, and exploitation. If the integrity of the COMSEC system is weakened at any point, all the sensitive information protected by that system may be compromised. Even more damaging, this loss of sensitive information may never be detected. The procedural safeguards placed on COMSEC equipment and materiel, covering every phase of their existence from creation through disposition, are designed to reduce or eliminate the possibility of such compromise.

Communications Security (COMSEC) is the general term used for all steps taken to protect information of value when it is being communicated. COMSEC is usually considered to have four main components: transmission security, physical security, emission security, and cryptographic security. Transmission security is that component of COMSEC which is designed to protect transmissions from unauthorized intercept, traffic analysis, imitative deception, and disruption. Physical security is that component of COMSEC, which results from all physical measures to safeguard cryptographic materiel, information, documents, and equipment from access by unauthorized persons. Emission security is that component of COMSEC which results from all measures taken to prevent compromising emanations from cryptographic equipment or telecommunications systems. Finally, cryptographic security is that component of COMSEC which results from the use of technically sound cryptosystems, and from their proper use. To ensure that telecommunications are secure, all four of these components must be considered.

Part of the physical security protection given to COMSEC equipment and materiel is afforded by the special handling it receives from distribution and accounting. There are two separate channels used for the handling of such equipment and materiel: "COMSEC channels" and "administrative channels." The COMSEC channel, called the COMSEC Materiel Control Systems (CMCS) is used to distribute accountable COMSEC items such as keying materiel, maintenance manuals, and classified and unclassified CCI equipment. (EXCEPTION: Some military departments have been authorized to distribute CCI equipment through their standard logistics system.) The CMCS channel is composed of a series of COMSEC accounts, each of which has an appointed COMSEC Account Manager who is personally responsible and accountable for all COMSEC materiel charged to the account. The COMSEC Account Manager assumes responsibility for the materiel upon receipt and then controls its dissemination to authorized individuals on a need-to-know basis. The administrative channel is used to distribute COMSEC information and materiel other than that which is accountable in the CMCS.

Particularly important to the protection of COMSEC equipment and materiel are an understanding of all security regulations and the timely reporting of any compromise, suspected compromise, or other security problem involving this materiel. If a COMSEC system is compromised but the compromise is not reported, the continued use of the system, under the incorrect assumption that it is secure, can result in the loss of all information that was even protected by that system.

If the compromise is reported, steps can be taken to change the system, replace the keying materiel, etc., to reduce the damage done. In short, it is your individual responsibility to know and to put into practice all the provisions of the appropriate publications, which relate to the protection of the COMSEC equipment and materiel to which you will have access.

Public disclosure of any COMSEC information is not permitted without the specific approval of your Government contracting office representative, DON Service authority (NCMS), or the National Security Agency (NSA). This applies to both classified and unclassified COMSEC information and means that you may not prepare newspaper articles, speeches, technical papers, or make any other "release" of COMSEC information without specific Government approval.

The best personal policy is to avoid any discussions, which reveal your knowledge of, or access to COMSEC information, and thus avoid making yourself of interest to those who would seek the information you possess.

You must know that should you willfully disclose or give to any unauthorized persons any of the classified, unclassified, or CCI COMSEC equipment, associated keying materials, or other COMSEC information to which you have access, you will be subject to prosecution under the Uniform Code of Military Justice and/or the applicable criminal laws of the United States. The laws that apply are contained in Sections 793, 794, and 798 of Title 18, United States Code.

Finally, any attempt to elicit the COMSEC information you have, either through friendship, favors, or coercion, must be reported immediately to your security office.

BRIEFING ACKNOWLEDGED THIS _____ DAY OF _____, 20_____

1. EMPLOYEE			
a. SIGNATURE	b. NAME (Last, First MI)	c. GRADE	d. EMPLOYEE/ DOD ID# (IF UNABLE TO DIGITALLY SIGN)
2. ADMINISTERING OFFICIAL			
a. SIGNATURE	b. NAME (Last, First MI)	c. GRADE	d. OFFICIAL POSITION

NOTE: (U) PRIVACY ACT STATEMENT: **The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the subject individual, unless the disclosure is pursuant to one of 12 statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.** Authority for collecting the requested information is contained in Executive Order 9397, Executive Order 12333 and Executive Order 12356.

(CUI) Notice: - This transmission contains material covered by the Privacy Act of 1974 and should be viewed only by personnel having an official "need to know". Any misuse or unauthorized disclosure may result in both civil and criminal penalties.

DEBRIEFED/ ACCESS REMOVED ON:	**RETAIN UNTIL/ DESTROY ON:**