CONTROLLED CRYPTOGRAPHIC ITEM (CCI) BRIEFING

1. As a member of a U.S. military service, agency, department, contractor or an authorized service vendor you have been selected to perform communications electronic maintenance and/or logistic support duties which will require access to sensitive communications security (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 written briefing will provide you with a description of the types of COMSEC information you 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 may incur for willful disclosure of this information to unauthorized persons. In addition, signing of this form indicates that you have received the required COMSEC security awareness training to a level commensurate with your level of involvement with the COMSEC components, equipment or systems.

2. COMSEC equipment is especially sensitive because it is used to protect other information against unauthorized access during the process of communicating that information from one point to another. Any piece of cryptographic equipment, keying or other cryptographic material may be the critical element that protects large amounts of sensitive/classified information from exploitation. If the integrity of the cryptographic system is weakened at any point, all the sensitive information protected by the system may be compromised; even more damaging, this loss of sensitive/classified information may never be detected. The procedural safeguards placed on cryptographic equipment and material, that covers every phase of their existence from design through disposition, are designed to reduce or eliminate the possibility of compromise.

3. 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 parts: 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 part of COMSEC which results from all physical measures to safeguard cryptographic equipment and materials from access by unauthorized persons. Emissions security is that component of COMSEC which results from all measures taken to prevent compromising emanations from cryptographic equipment or telecommunications equipment. 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.

4. Part of the physical security protection given to COMSEC equipment and material is afforded by its special handling and accounting. There are two separate channels used for the handling of such equipment and materials: "the COMSEC channel" and "the administrative channel." The COMSEC channel, called the COMSEC Material Control System, is used to distribute accountable COMSEC items such as classified and CCI equipment, keying material, and maintenance manuals (EXCEPTION: Some Military Departments have been authorized to distribute CCI equipment through their standard logistics system). This channel is composed of a series of COMSEC accounts, each of which has an appointed COMSEC Custodian who is personally responsible and accountable for all COMSEC materials charged to his account. The COMSEC Custodian assumes accountability for the equipment or material upon receipt, then controls its dissemination to authorized individuals on job requirements and a need-to-know basis. The administrative channel is used to distribute COMSEC information other than that which is accountable in the COMSEC Material Control System.

5. Particularly important to the protection of COMSEC equipment and material is an understanding of their security regulations and timely reporting of any compromise, suspected compromise or other security problems involving COMSEC equipment or materials. If a COMSEC system is compromised, but the compromise is not reported, the continued use of the system, under the assumption that it is secure, can result in the loss of all information that was ever protected by the system. By reporting the compromise, steps can be taken to change the system, replace the key, etc., to reduce the damage. In short, it is your individual responsibility to know and put into practice all the security provisions which relate to the protection of the COMSEC equipment and material to which you will have access.

6. Public disclosure of any COMSEC information, other than those specific cases discussed in the Government Contractors Controlled Cryptographic Item (CCI) Manual is not permitted without the specific approval of your Government contracting office representative or the National Security Agency (NSA). This applies to both classified and unclassified cryptographic information, and means that you may not prepare newspaper articles, speeches, technical papers, or make any other "release" of cryptographic information without specific Government approval. The best personal policy is to avoid any discussions which reveal your knowledge of or access to cryptographic information and thus avoid making yourself of interest to those who would seek information you possess.

7. Finally, you must know that should you willfully disclose or give any unauthorized persons any of the cryptographic equipment, keying material, or other cryptographic materials or information to which you have access, you may be subject to prosecution under the criminal laws of the United States. The laws which apply are contained in Title 18, United States Code, sections 641, 793, 798, and 952.

8. If your duties include access to classified COMSEC equipment, information, or material in addition to the above, you should avoid travel to any countries which are adversaries of the United States, or their establishments/facilities within the U.S. Should such travel become necessary, however, your security office should be notified sufficiently in advance so that you may receive a defensive security briefing. Any attempt by a person or persons to elicit the classified COMSEC information you have, either through friendship, favors, or coercion must be reported immediately to your Security office.

9.a. NAME *(Last, First, Middle Initial) (Typed or printed)*		**10**.a. INSTRUCTOR/BRIEFED BY *(Typed or printed name - Last, First, Middle Initial)*	
b. SIGNATURE	c. DATE SIGNED	b. SIGNATURE	c. DATE SIGNED