STU-III Briefing

Listed are some procedures and guidelines that must be adhered to when assigned the responsibility of caretaker or when using the STU-III.

A. The STU-III is categorized as being a Controlled Cryptographic Item (CCI), i.e., secure telecommunications or information handling equipment, or associated cryptographic component, which is unclassified but controlled.

1. Secure Telecommunications and Information Handling Equipment is defined as equipment designed to secure telecommunications and information handling media by converting information to a form unintelligible to an unauthorized interceptor and by reconverting the information to its original form for authorized recipients. Such equipment, employing a classified cryptographic logic, may be stand-alone crypto-equipments as well as telecommunications and information handling equipments with integrated or embedded cryptography.

2. Cryptographic Component is defined as the hardware or firmware embodiment of the cryptographic logic in a secure telecommunications or information handling equipment. A cryptographic component may be a modular assembly, a printed circuit board, a microcircuit, or a combination of these items.

B. Storage and Transportation of CCI equipment: CCI equipment and components shall be stored and transported in a manner that affords protection at least equal to that which is normally provided to other high value/sensitive material, and ensures that access and accounting integrity is maintained.

C. Access: A security clearances is not required for access to the STU-III. However, access shall be restricted to U.S. citizens whose duties require such access. Access may also be granted to permanently admitted resident aliens who are U.S. government civilian employees or active duty or reserve members of the U.S. Armed Forces whose duties require access.

D. An unkeyed STU-III may be used for unclassified or nonsensitive calls. It must be treated and protected as other sensitive, high-value items, (i.e., a personal computer, typewriter, or telecopier).

E. A keyed STU-III must be afforded protection commensurate with the classification of the key it contains. When persons in an area are not cleared to the level of the keyed terminal, it must be under the operational control and within view of at least one appropriately cleared, authorized person.

1. Adhere to the security classification on the display. For example, if the display says SECRET, you may not talk above the SECRET level.

2. When secure calls are placed using STU-IIIs, the common sense approach must be used to prevent unauthorized personnel from overhearing a classified or sensitive phone conversation. Such measures as escorting unauthorized personnel out of the area and closing room and hallway doors should be taken.

3. Check the display for any discrepancies or failures and report them to the COMSEC Custodian immediately.

4. If someone with a clearance below the level of the crypto key being used desires to make a call, the CIK and the call must be monitored by another person who has a clearance equal to or above the level of the crypto key. (Example: If your STU-III is keyed at the TOP SECRET level and person using your unit has a SECRET clearance, you must activate the call and advise the party being called that the conversation must be kept at the SECRET level.)

F. Accountable COMSEC material issued on a hand receipt will never be reissued by a user. If material is needed by another individual other that the immediate office of the original recipients, the material must be returned to the COMSEC custodian for reissue.

G. The responsibility for maintaining security and control of material received on a hand receipt from the custodian remains until the custodian relieves the individual by returning the signed receipt to the initial recipient.

System Security Guidance

A. Protection of Crypto Ignition Key (CIK): The individual assigned the responsibility of accepting and signing for the CIK is ultimately responsible for the security of the CIK and maintaining the integrity of the National Security System involved.

1. The need to know and security clearance of any individual requesting the usage of the CIK must be validated prior to allowing them access to the CIK and instrument.

2. Individuals with security clearances are not automatically entitled to access of classified information.

B. Movement of STU-IIIs: STU-IIIs will not be moved from their original installation location without prior approval of the issuing COMSEC Custodian, or in his absence, the Department COMSEC Custodian.

C. Secure STU-II Data Applications: Prior to using the STU-III for secure data applications, authorization must be received from NC. Guidance will be provided upon request/notification that requirements exist for using this feature of the phone.

D. STU-III Travel Restrictions: The Telecommunication Management Division (TMD) of DOC will be notified in advance of plans to use the STU-IIIs on travel. Those persons going on travel will be briefed on protecting the instrument while on travel. Only unclassified/sensitive key will be used while on travel. Classified key requirements for travel will be reviewed on a case-by-case basis. Requirements involving classified key must arrive in TMD at least 21 working days in advance of travel date (this allows time to order the key). Only STU-IIIs with an appropriate carrying case that have been designated as a mobile nit will be used on travel.

E. Installed in Residence/Automobile: Terminals installed in the residence or automobile should be used only by those persons for whom it is installed. All of the security requirements should be observed for preventing unauthorized access in the keyed terminal and to classified and sensitive information. The CIK should be removed from the terminal following each use and kept in the personal possession of the user, or properly stored. If the CIK is stored in the residence or automobile and the associated terminal is used to protect classified information, the CIK should be protected in an approved security container.

F. Violations: You may be particularly aware of these security issues when making a secure call. Deviations from any of the above could result in a violation or constitute a practice dangerous to security and lead to serious consequences, such as, written reprimand, letter of counseling, or the loss of job.

By signing the certification sheet below you are indicating that you have read and understand all of the above.

My signature below indicates that I have read/been briefed and understand the Department of Commerce, Office of Security STU III Briefing. I am aware that any questions I have concerning the contents of this briefing should be directed to my Regional Security Officer.

PRINT NAME_____

SSN_____

BUREAU/OFFICE_____

TRAVEL DATE(S)_____

COUNTRY(IES)/REGION_____

WORK PHONE _____

_____
SIGNATURE DATE

Collection of this information is authorized by Executive Order 9397, 10450, 12356, U.S.C. 301 and 7531-532; 15 U.S.C. 1501 et seq; AND 44 U.S.C. 3101

Please forward this signed page to the following:

REGIONAL SECURITY OFFICE
7600 SAND POINT WAY NE
SEATTLE, WA 98115-6349
Fax 206-526-4543