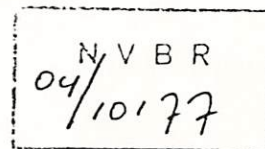


NATO RESTRICTED

89 OKI. 1309

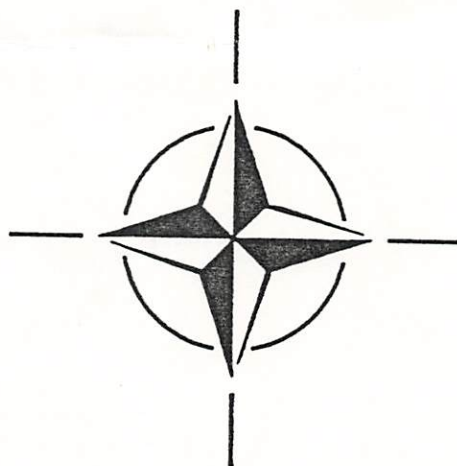
SDIP-8



OPERATIONAL COMSEC DOCTRINE

For The

SPENDEX-40 (NU)



NATO RESTRICTED

NATO RESTRICTED

SDIP-8

14 AUG 1989

FOREWORD

1. This publication, Operational COMSEC Doctrine for the SPENDEX-40, prescribes minimum standards for the safeguarding and control of the SPENDEX-40 cryptosystem and related COMSEC material. It is effective upon receipt.

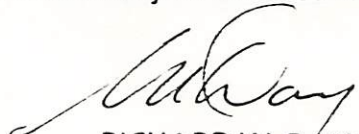
2. The provisions of this publication are prescriptive. Requests for waivers to any of its provisions must be submitted to SECAN.

3. When this doctrine addresses communication between SPENDEX-40 in KDC or NET00 modes, the procedures equally apply to communication between SPENDEX-40 and KY-71A.

4. Responsibility for distributing this document to their subordinate elements rests with the Major NATO Commands, NATO National Ministries of Defense, or the Chiefs of the Military Services.

5. Extracts from this publication may be made for official purposes. Additional copies may be requested from SECAN, and the entire publication may be duplicated locally without SECAN authorization.

6. This publication in its entirety is classified NATO RESTRICTED.



RICHARD W. DAY
Director
SECAN and DACAN

CLASSIFIED BY C-M(55)15(FINAL)
DECLASSIFY ON: ORIGINATING
AGENCY'S DETERMINATION REQUIRED

NATO RESTRICTED

NATO RESTRICTED

SDIP-8

OPERATIONAL COMSEC DOCTRINE FOR THE SPENDEX-40

	<u>SECTION</u>
PURPOSE	I
PROMULGATION	II
REFERENCES	III
DEFINITIONS	IV
SYSTEM COMPONENTS	V
APPLICATION	VI
CLASSIFICATION	VII
KEYING	VIII
CRYPTOPERIODS	IX
CRYPTONET SIZE	X
PHYSICAL SECURITY	XI
EMERGENCY PROCEDURES	XII
REPORTABLE COMSEC	
COMPROMISES AND VIOLATIONS	XIII
ACTIONS FOR COMPROMISE	
RECOVERY	XIV

SECTION I - PURPOSE

1. This document prescribes the COMSEC doctrine for operational use of the SPENDEX-40 Secure Telephone and associated keying material and documentation within NATO.

SECTION II - PROMULGATION

2. The doctrine contained in this document should be made available to all organizations associated with NATO which plan to use SPENDEX-40 equipment.

SECTION III - REFERENCES

3. Reference Listing:

- a. C-M(55)15(FINAL), "Security Within the North Atlantic Treaty Organization, dated 31 July 1972.
- b. AMSG 293, "NATO Cryptographic Instructions."
- c. AMSG 505, "NATO CRYPTO Distribution and Accounting Publication."
- d. AMSG 524, "NATO Glossary of Communications Security Terms."

NATO RESTRICTED

SDIP-8

e. AMMSG 725, "Controlling Authorities for Crypto Keying Material and Management of Manual Cryptosystems."

SECTION IV - DEFINITIONS

4. Definitions contained AMMSG 524 apply to this instruction except as follows:

Controlled Cryptographic/COMSEC Item (CCI): An unclassified but controlled secure telecommunications or automated information handling equipment and associated cryptographic assembly, component, or other hardware or firmware item that performs a critical COMSEC or COMSEC-ancillary function. NOTE: CCIs are marked "CONTROLLED CRYPTOGRAPHIC ITEM" or, where labeling spaces requires, "CCI."

SECTION V - SYSTEMS COMPONENTS

5. The SPENDEX-40 is used in conjunction with the NATO Key Distribution Center (KDC-II) to provide secure telephone service to all narrowband secure voice users. The following items are used at user locations, although not all items are used at all locations:

a. SPENDEX-40 Secure Telephone Unit: The SPENDEX-40 contains the voice and signal processing circuitry and cryptographic circuitry necessary for encryption and decryption of voice and data transmissions.

b. Crypto-Ignition Key (CIK): Must be plugged into the SPENDEX-40 whenever it is being keyed and when making or receiving a secure call.

c. KOI-18 General Purpose Tape Reader: Used to load hard-copy key tapes into the KYK-13 or SPENDEX-40.

d. KYK-13 Electronic Transfer Device: Used to load electronic keys into a SPENDEX-40.

NOTE: The SPENDEX-40 has an additional keying capability. For further information, contact the Netherlands National Communications Agency, The Hague.

NATO RESTRICTED

SDIP-8

SECTION VI - APPLICATIONS

6. The SPENDEX-40 is capable of operating in the Key Distribution Center (KDC) mode and the net (NET00) mode.

a. KDC mode: SPENDEX-40 terminals associated with the NATO KDC are self-authenticating to the NATO SECRET level and can pass information which is classified to that level. All NATO SPENDEX-40 operational keying material (KDC and net) is classified NATO SECRET. For COSMIC TOP SECRET and Special Category Information, a sound-proof booth/office, that is subject to regular technical security inspections, should be used as well as to use appropriate authentication systems.

b. NET00 mode (equivalent to KY-71A net mode): SPENDEX-40 terminals which operate in the NET00 mode, as isolated cryptonets using key material of the appropriate classification, are self-authenticating to the NATO SECRET level.

NOTE: Users must be aware that a SPENDEX-40 receiving a secure call automatically switches to the mode (KDC or NET00) of the calling party. When the called SPENDEX-40 equipment is initializing to the SECURE mode, the display indicates momentarily which key system is used: "**EKD" in case of KDC mode, and "**EMG" in case of NET00 mode. Users relying on the use of NET00 key to self-authenticate incoming calls to the NATO SECRET level must ensure that their SPENDEX-40 is operating in the NET00 mode ("**EMG" momentarily in display) for each such call.

SECTION VII - CLASSIFICATION

7. Classification:

a. Reports: Technical, operational, and project reports dealing with the SPENDEX-40 must be classified by their originators on the basis of content. In general, detailed information relating to the cryptographic capabilities of SPENDEX-40 equipments must be classified at least NATO CONFIDENTIAL. Information concerning all cryptanalytic or TEMPEST vulnerabilities of this equipment must be classified at least NATO SECRET.

b. Equipments:

(1) SPENDEX-40

(a) with CIK: SPENDEX-40 assumes the highest classification of the key stored, minimum NATO CONFIDENTIAL

(b) without CIK: UNCLASSIFIED CCI

(2) The CIK is classified NATO CONFIDENTIAL.

NATO RESTRICTED

SDIP-8

(3) KOI-18 general purpose tape readers, and unkeyed KYK-13 electronic transfer devices are CCI's.

(4) Handling of keyed SPENDEX-40 equipment and KYK-13s must be consistent with the classification of the highest classified cryptovariable stored therein.

(5) Photographs, diagrams, and drawings of SPENDEX-40 equipment must be marked at least NATO RESTRICTED.

(6) The SPENDEX-40 equipment is UNCLASSIFIED for external viewing, provided all covers are in place.

c. Keying Material: NATO operational KDC mode key material and NET00 mode key material is classified NATO SECRET) NATO on-the-air training and test key material is classified NATO CONFIDENTIAL. All of these types of key tape are marked "CRYPTO" and are packaged in protective canisters; special safeguarding instructions for them are contained in associated handling instructions.

d. Supporting Documentation: The following documentation will be used with the SPENDEX-40:

(1) SPENDEX-40 interim repair procedure

(2) 9922-154-12551, Subject: Operating Instructions for
SPENDEX-40

(3) 9922-154-12561, Subject: Installation and COMSEC Manual

e. Release of Information: The unrestricted dissemination of NATO UNCLASSIFIED COMSEC information, particularly that related to crypto-equipment, is prohibited. Photographs, drawings, or descriptive information for press release or private use are prohibited. The open or public display of the SPENDEX-40 or its components at nongovernmental symposia, meetings, open-house tours, or for other nonofficial purposes is forbidden. This prohibition includes discussion, publication, or information pertaining to the SPENDEX-40 for other than official purposes. A security clearance is not required for casual viewing of SPENDEX-40 equipment, such as may occur when installed in a user's office.

SECTION VIII - KEYING

8. Keying:

a. Cryptovariables: The following types of cryptovariables are used with the SPENDEX-40:

(1) Unique Cryptovariable (Vu). The Vu is a hard-copy key encryption key (KEK) unique to each individual SPENDEX-40. It is used only for protecting per-call cryptovariables (Vcalls) and is held only at the SPENDEX-40 and the KDC-II. The Vu is never used to protect traffic. A SPENDEX-40 Vu may be

NATO RESTRICTED

NATO RESTRICTED

SDIP-8

updated only by operator action at the SPENDEX-40. Whenever a SPENDEX-40 is updated, a simultaneous update must be done at the KDC-II in order for the SPENDEX-40 to continue to operate in the KDC mode. Individual Vus may not be used at more than one terminal without the specific prior approval of SECAN.

(2) Per-Call Cryptovisible (Vcall). The Vcall is a traffic encryption key (TEK), electronically generated by a KDC-II. A Vcall is generated upon request of the calling SPENDEX-40 and is transmitted in encrypted form to the calling SPENDEX-40, which then automatically transmits it to the called SPENDEX-40. The Vcall protects traffic between these two SPENDEX-40s, and is not retained by the KDC-II. Up to 20 Vcalls, protected by the Vus, can be stored in a SPENDEX-40 and used for subsequent calls to the same SPENDEX-40. Since the distribution of the Vcall is so limited, and the Vcall appears only in electronic form, its use provides the most secure SPENDEX-40 operating mode.

(3) NET00 Cryptovisible (Vn). The Vn is a hard-copy TEK held by the members of NATO cryptonets whose terminals operate in the NET00 mode (is equivalent to the KY-71A net mode). Vns are intended for two purposes. The contingency Vn is intended to provide a back-up capability to allow for secure communications among SPENDEX-40s when no stored Vcalls are available and communication with the KDC-II is disrupted or KDC-II service is otherwise not available. The community of interest Vn is the net mode key material used by discrete communities of interest who operate outside the NATO KDC structure in nets which self-authenticate to the NATO SECRET level. Vns are classified NATO SECRET.

b. Key Tapes: Vus and Vns are generated by DACAN and provided in punched tape form. They may be loaded into a SPENDEX-40 using a KOI-18 alone or in combination with a KYK-13.

c. Crypto-Ignition Key (CIK): The SPENDEX-40 employs a split key concept involving a physical device referred to as a crypto-ignition key (CIK). After loading the first cryptovisible in a zeroized or "empty" SPENDEX-40 CIK combination, the plugged CIK is made "valid" for that SPENDEX-40. This "valid" or associated CIK must be plugged into the SPENDEX-40 whenever cryptovisibles are loaded or the secure mode of the SPENDEX-40 is activated. When the associated CIK is removed the SPENDEX-40 can operate only in the nonsecure (clear) mode, and the SPENDEX-40 reverts to being CCI. When the associated CIK is plugged into the SPENDEX-40, the SPENDEX-40 is considered to be keyed and assumes the highest classification of the cryptovisibles stored.

SECTION IX - CRYPTOPERIODS

9. The cryptoperiods for the SPENDEX-40 cryptovisibles are as follows:

a. Vu. Three months. The controlling authority may authorize extensions of up to seven days. Vus will be updated whenever directed by the controlling authority either to facilitate recovery from a compromise, or in special circumstances where there is a high risk of loss of a keyed terminal where back traffic must be protected, e.g., an embassy facing overrun.

NATO RESTRICTED

b. Vcalls. One call, or may be stored and used for all calls to the same SPENDEX-40 for the length of the Vu cryptoperiod, if the identification number of the called SPENDEX-40 associated with a specific Vcall has been included in the memory of 20 stored Vcalls.

c. Vn. One month. The controlling authority may authorize extensions of up to 48 hours. It is essential for the maintenance of security for that effective Vns be updated daily at all SPENDEX-40s. To ease the operational burden, Vn updates need not be carried out on weekends or holidays when the SPENDEX-40 is not used, however, Vns must be updated at all SPENDEX-40s at least once a week. Failure to do so is a reportable insecurity. As an exception, the controlling authority for a Vn may waive the weekly update requirement for specific installations where the user may be absent for longer than one week, e.g., residence installations, provided that the CIK is returned to the cryptocustodian or other separate secure facility for safekeeping and the Vn is updated immediately after the CIK is returned to the user. Because Vns are superseded monthly, daily updating will result in the effective Vn update setting matching the calendar day of the month, i.e., Setting 1 is used on the first of the month, Setting 2 on the second, etc. Vn updates must be done at the SPENDEX-40 using the local update procedure.

d. CIK update. The CIK in operational use must be updated at least once a week by making a secure call.

SECTION X - CRYPTONET SIZE

10. The cryptonet size limitations for the SPENDEX-40 cryptovariabls are as follows:

a. Vu: One SPENDEX-40 and the KDC-II.

b. Vcall: Two SPENDEX-40s. (The KDC-II generates Vcalls, but does not retain them once they have been transmitted to the SPENDEX-40s)

c. Vn: As determined by the controlling authority, Vns may be used in contingency and other applications. The following guidance applies:

(1) Contingency Vns. In the event of a failure of the Vcall mode affecting a community of secure voice subscribers, the controlling authority can activate a contingency Vn mode of operation. The contingency Vn cryptonet should be kept to the minimum number of holders necessary to support essential communications.

(2) Other Vns. Cryptonets for other, noncontingency, communications applications should be kept as small as possible to minimize the risk and impacts of a Vn compromise. Vn cryptonets among SPENDEX-40s involved in long distance calls (most likely using microwave or satellite communications links), and multiple cryptoaccounts (where more people are involved in Vn distribution), are more vulnerable to intercept and increased risk of HUMINT exploitation. Vn cryptonets, other than contingency cryptonets, should not be larger than 30 holders. Exceptions to any of the above community of interest Vn

application or cryptonet size restrictions may be approved by the Vn controlling authority on a case-by-case basis. A copy of all such approvals shall be provided to SECAN for information.

SECTION XI - PHYSICAL SECURITY

11. The SPENDEX-40 is designed for use in offices and residences where no more than a low level of physical security can be provided. The removable CIK is the feature that permits relaxing normal physical security requirements. Should either the SPENDEX-40 or the associated (or valid) CIK be individually compromised, the encrypted conversations or data traffic would still remain secure. An enemy must compromise both the keyed SPENDEX-40 and the associated CIK, or the key tape alone, in order to recover plain text. The key to the security of SPENDEX-40 protected traffic is the provision of separate protection for the SPENDEX-40 and its associated CIK, thus forcing an enemy to make two separate physical penetrations to recover the operational SPENDEX-40 cryptovariables. SPENDEX-40 may be installed wherever it is necessary to provide secure voice service to NATO officials. Of course, it remains the responsibility of the users to ensure that classified conversations are not vulnerable to eavesdropping.

a. Access, Storage and Transportation: Uninstalled SPENDEX-40, supporting cryptographic equipment and components, keying material, and associated classified documentation shall be safeguarded in accordance with the access, storage and transportation requirements of AMMSG-293 and AMMSG-505.

b. Requirements for SPENDEX-40 Facilities: An installed SPENDEX-40 without CIK must be protected to a degree which, in the judgment of the responsible commander or civilian official, 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. SPENDEX-40 may be installed in a variety of locations in order to meet users' legitimate requirements for secure voice service. If the SPENDEX-40 is to remain keyed (i.e. with CIK installed), the requirements of paragraph 11.f. below apply. When the facility is no longer occupied by appropriately cleared personnel, the CIK must be removed from the SPENDEX-40 and provided separate protection in accordance with the requirements of paragraph 11.e. below. Since conditions differ from site to site, it is not feasible to prescribe a single set of physical security controls for all SPENDEX-40s, but generally, an office space secured with a deadbolt lock will provide sufficient protection. If there is a high risk of theft in a specific installation, then additional security measures such as guards, alarms, substantial construction, or use of the optional SECAN-approved security container, may be appropriate. These protective measures are intended to allow the installation of SPENDEX-40 in areas now approved for classified discussions and the storage of high value/sensitive equipment without changes to either construction of the area or access to it. Although the vulnerability to technical surveillance remains, the addition of the SPENDEX-40 into an area does not appreciably change that vulnerability.

c. Installation in Residences: Installation of SPENDEX-40s in the residences or quarters of military or civilian officials may be authorized on a case-by-case basis by the NATO Office of Security (NOS) or his delegated authority. There is no general requirement to store the SPENDEX-40 in a security container. However, in cases where there is a threat of penetration or a physical security problem, the SPENDEX-40 should be stored in a SECAN-approved optional security container. Each installation must be evaluated on its individual security merits since most residences do not provide a high degree of inherent security. For this reason, placing a secure telephone in a residence may involve taking some risks to satisfy the operational requirements of the user. These risks can be minimized by effectively controlling the CIK, preferably by keeping it on the person of the authorized user when away from the residence. A less desirable alternative is to store the CIK in a SECAN-approved security container within the residence. It is preferable to keep it separate from the SPENDEX-40 in order to force an adversary at least to spend time searching for it. The CIK may not be stored in the same container as the SPENDEX-40, unless the user is in the residence at the time. If the residence is to be unoccupied for more than three days, or the user is to be absent for more than seven days, the SPENDEX-40 shall be removed and provided separate secure storage. This provision may be waived by the cognizant security authority if the unoccupied residence is considered adequately secure to preclude any reasonable chance of theft. Users should be aware of the vulnerability of their residences to clandestine electronic surveillance.

d. Safeguarding:

(1) A SPENDEX-40 and a commercial telephone desk set may be collocated and both may be placed on the same metal surface without causing a TEMPEST problem. However, collocation of a SPENDEX-40 and commercial telephone desk set may contribute to an audio security problem. Consult your own security office for guidance on the approved types of models, installation requirements, and recommended locations of all commercial telephones in the vicinity of a SPENDEX-40.

(2) Used in combination with classified data processing equipment (data mode) the SPENDEX-40 should be separated at least one meter from all other equipment and lines.

e. Protecting the SPENDEX-40 CIK: The CIK is NATO CONFIDENTIAL. The CIK must be properly plugged into its associated SPENDEX-40 in order to activate the secure mode of the SPENDEX-40. (NOTE: An operational CIK is a CIK which contains a random word, previously generated by the SPENDEX-40, which, when added to the contents of the key storage registers of the associated SPENDEX-40, regenerates the cryptovariables stored within that SPENDEX-40). When removed from the SPENDEX-40, the CIK shall be protected as follows:

NATO RESTRICTED

SDIP-8

(1) Retained under the personal control of a authorized user. The CIK may be taken along whenever the authorized user leaves the office. It should be protected as NATO CONFIDENTIAL. For example, it may be kept under direct personal control in a pocket or purse. Common sense should be used in protecting the CIK in the higher threat areas.

(2) Stored in a locked container in an area separate from the SPENDEX-40. An approved security container should be used, if available, but a key-locked desk or cabinet may be used if necessary.

(3) Stored in a centralized key desk protected full time.

(4) Stored in the same area as the SPENDEX-40 only if it is kept within a security container approved for storage of NATO SECRET keying material, unless the entire area is a vault or controlled area approved for the open storage of NATO SECRET keying material. Secure storage is required in this situation since the CIK need only be inserted into the SPENDEX-40 in order to key the terminal with the NATO SECRET keying material. Thus, storage of the CIK in the same area as the SPENDEX-40 is equivalent to leaving the terminal keyed.

f. Protection of Keyed SPENDEX-40: Keyed SPENDEX-40 equipment (with CIK installed) must be protected in accordance with the highest classification of the keys stored (see para 7.c). Protection of the keyed terminal at the NATO SECRET level may be a serious operational problem. Whenever a keyed, operational SPENDEX-40 is to be left unattended by all authorized terminal users, the CIK should be removed and appropriately stored or taken along by the last authorized user to leave the facility. Key tapes classified NATO SECRET must remain in the custody of NATO SECRET cleared personnel. When left unattended by all cleared personnel, keyed terminals must be locked in approved security containers or installed in areas approved for the open storage of NATO SECRET material.

g. Handling of Key Material: The SPENDEX-40 keying material is most vulnerable to HUMINT exploitation after it has been removed from the canister and while it is held in electrical form in KYK-13s. In order to limit access as much as possible to the keying material, the procedures outlined below will be followed:

(1) Key tapes will be kept within their protective canisters until shortly before they are to be used. Canisters may be issued to users or maintenance personnel for rekeying, but should be returned to the cryptocustodian immediately after use for secure storage. Users should not normally retain possession of key tape canisters, except in special circumstances, such as when user locations are isolated and difficult to reach. Key tape canisters contain multiple copies of the same keying material to support SPENDEX-40 rekeying during a cryptoperiod.

(2) Key tape segments, once removed from a protective canister, will be destroyed as soon as possible after they have been used to successfully load a SPENDEX-40 or KYK-13. As an exception, when the immediate destruction cannot be witnessed, the key tape may be retained for that purpose, but in no case will destruction be delayed more than 12 hours from the time the terminal is successfully keyed. This means that personnel using the tapes to load the SPENDEX-40 will normally destroy the tapes at the site, unless the tapes can be immediately hand-carried back to the cryptocustodian after the successful loading of the SPENDEX-40. All tape segments, used or not, must be destroyed at the end of each cryptoperiod with the exception that the last tape segment in the canister may be kept until new cryptovariable is successfully loaded at the beginning of the new cryptoperiod and then destroyed. The KYK-13 must be zeroized after loading the SPENDEX-40.

SECTION XII - EMERGENCY PROCEDURES

12. An Emergency Protection Plan should be prepared in accordance with the guidance of AMMSG-293. The standard priority for destruction of COMSEC material should be followed for SPENDEX-40 COMSEC material, with the following additions:

a. Operational CIK: The operational CIK should be zeroized by zeroizing the SPENDEX-40 with or without the CIK when it is no longer necessary to maintain secure communications.

b. Temporary Abandonment of a SPENDEX-40: If an operational SPENDEX-40 is to be temporarily abandoned, it need not be zeroized; however, the operational CIK should be evacuated by authorized personnel. If it is later determined that the SPENDEX-40 will not be recovered, the operational CIK should be zeroized by plugging it into any usable SPENDEX-40 and pressing the zeroize button.

WARNING: The SPENDEX-40 used is completely zeroized too.

SECTION XIII - REPORTABLE COMSEC COMPROMISES AND VIOLATIONS

13. A general listing of reportable COMSEC compromises and violations and the standards for their reporting are contained in AMMSG-293. Additional compromises and violations specific to the SPENDEX-40 follow:

a. Reportable Cryptographic Violations:

(1) Use of a contingency Vn without the prior authorization of the controlling authority.

(2) Failure to update an effective Vn at least once a week, unless an exception has been approved by the controlling authority.

b. Reportable Physical Compromises and Violations:

- (1) Unauthorized, unescorted operational use of a SPENDEX-40.
- (2) Unauthorized extraction or loading of key material.

SECTION XIV - ACTIONS FOR COMPROMISE RECOVERY

14. The following special guidance applies to actions to be taken to recover from a compromise involving SPENDEX-40 COMSEC material, in addition to the normal actions of emergency supersession, reduced use pending supersession, etc.

a. Loss of an Operational CIK: When an operational CIK is lost, it must be reported as a possible insecurity. The SPENDEX-40 must be zeroized and cannot be used as a secure instrument until rekeyed with new cryptovariables. The act of terminal zeroization makes the lost CIK useless.

b. Loss of a Keyed SPENDEX-40 and its CIK: Loss of a keyed SPENDEX-40 and its CIK, as might happen during the overrun of a fixed facility, creates a special set of security problems. The immediate danger is that calls to or from the terminal may be used to deceive other system users. The controlling authority, upon notification of the loss of a keyed SPENDEX-40, is not required to notify all SPENDEX-40 users to update their Vus due to the extreme difficulty of accomplishing this action without a serious disruption in secure communications. The controlling authority, however, shall take the following actions, in priority order:

(1) Notify operators at the KDC-II to take immediate action to delete the identification number of the compromised terminal from the KDC-II data base. This action will preclude the compromised terminal from receiving new Vcalls from the KDC-II.

(2) Notify all secure voice users of the telephone directory listing of the compromised terminal. The initial notification should go to those users most likely to have communicated with the compromised terminal. For unlisted numbers, special arrangements should be made between the using element and the controlling authority for compromise recovery actions. Upon becoming aware of the compromise, all terminal users having been involved in calls to or from that terminal, or having a Vn in common with the compromised terminal loaded into their terminal, must take action to notify their cryptocustodian. The cryptocustodian should then take immediate action to update the Vn of the affected secure voice equipment in coordination with the similar update action at the associated KDC-II, and, if applicable, request the Vn controlling authority to initiate supersession action. Users should be especially alert for deception attempts until all affected Vus are updated and compromised Vns are superseded.

1. The following information is being furnished to you for your information only.

2. This information is being furnished to you in confidence.

3. It is requested that you keep this information confidential.

SECTION 1. PURPOSE AND SCOPE

1. The purpose of this document is to provide information regarding the activities of the [redacted] and the [redacted] in the [redacted] area.

2. The scope of this document is limited to the activities of the [redacted] and the [redacted] in the [redacted] area.

3. The information contained in this document is for your information only and is not to be distributed outside your organization.

4. The information contained in this document is for your information only and is not to be distributed outside your organization.

5. The information contained in this document is for your information only and is not to be distributed outside your organization.