

CJCSI 6511.01
1 February 2001

**INFORMATION SECURITY
GUIDELINES FOR THE
DEPLOYMENT OF
DEPLOYABLE SWITCHED
SYSTEMS**



JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J6
DISTRIBUTION: A, B, C, J, S

CJCSI 6511.01
1 February 2001

INFORMATION SECURITY GUIDELINES FOR THE DEPLOYMENT OF DEPLOYABLE SWITCHED SYSTEMS

References: See Enclosure C.

1. Purpose. This instruction provides baseline guidance for the security of communications traffic that may be routed through deployable tactical switched systems forming joint task force (JTF) communications networks. It supplements references a through j. Information presented herein may address information/policies found in those references at enclosure c, and is restated in the context of the instruction not to supersede but to clarify.
2. Cancellation. None.
3. Applicability. This instruction applies to the Military Services, Joint Staff, combatant commands, and those activities and agencies reporting to the Chairman of the Joint Chiefs of Staff. The term "Military Services" as used herein refers to the US Army, US Navy, US Air Force, and US Marine Corps. It will apply to the US Coast Guard when the US Coast Guard forms part of a JTF and must interface its communications systems with those of the JTF network.
4. Policy. As stipulated in references a through i, DOD policy enjoins all DOD components to protect their operational activities against hostile intrusion through the application of information security (INFOSEC) measures. It is ultimately the responsibility of combatant and component commanders, however, to determine the degree of INFOSEC to be applied to tactical switched systems based on the risks found to be acceptable for the protection of their operations against hostile threats or other forms of potential disruption. The Joint Staff has the responsibility of providing basic guidelines that may aid combatant commanders in

chief and component commanders and can serve as a point of departure in meeting the security needs of joint formations. This responsibility applies to the deployable switches and related transmission systems of the tactical units that form and subscribe to JTF communications networks. The Joint Staff has established some basic guidelines with corresponding rules for the protection of communications traffic flowing through tactical switch systems and associated transmission media within JTF networks. Those guidelines are the rules specified in the procedures of this instruction.

5. Definitions. See Glossary.
6. Responsibilities. See Enclosure B.
7. Summary of Changes. None.
8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--<http://www.dtic.mil/doctrine>. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.
9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:



S. A. FRY
Vice Admiral, U.S. Navy
Director, Joint Staff

Enclosure(s):

- A - Procedures
- B - Responsibilities
- C - References
- GL - Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
.....	
Defense Information Systems Agency.....	10
Directorate for Command, Control, Communications, and Computer Systems	10
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	10
National Security Agency.....	10

(INTENTIONALLY BLANK)

ENCLOSURE A

PROCEDURES

1. Introduction. DOD policies in references a through h, and national policy in reference i establish requirements to deny unauthorized persons access to classified or unclassified-but-sensitive information while it is being electronically transmitted from a sender to a receiver. They also establish requirements to prevent the derivation of valuable information from other aspects of communications (such as traffic flow and message analysis) and to enhance the authenticity of communications.

a. Communications security (COMSEC) measures and controls are applied to the extent necessary to deny unauthorized persons information derived from US military telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security (TRANSEC), emission security, and the physical security of COMSEC material. COMSEC is a part of the general category of information security (INFOSEC). It provides for the protection of information systems against unauthorized information access or modification, whether the information is in storage, processing, or transit, and denies unauthorized user service.

b. As noted, TRANSEC is a component of COMSEC and results upon the application of measures designed to protect transmissions from interception and exploitation by a means other than cryptanalysis. Within the joint communications community, COMSEC often refers to the encryption of transmitted information that converts it from "RED" (classified) to "BLACK" (unclassified) before TRANSEC measures are applied. Thus, TRANSEC becomes an added measure of protection and is applied when the information being transmitted needs protection against two types of vulnerabilities that the network at risk faces, unauthorized data or information readability and traffic analysis. TRANSEC protects the information flow from traffic analysis or other network-level attack. In the case of unclassified information being passed along a specific path, TRANSEC measures may be the only protection needed. During the following discussion, "COMSEC" refers specifically to the encryption of voice, message, and data traffic.

2. General Practices. Telecommunications paths transmitting classified information will be secured by either National Security Agency (NSA)-endorsed equipment and keying material or by protected distribution systems (PDSs). Telecommunications paths transmitting unclassified-

but-sensitive information will be protected in a manner based on the magnitude of harm that could result from the information's unauthorized disclosure, loss, misuse, alteration, destruction, or nonavailability.

a. The use of encryption. NSA-approved encryption techniques may be used separately or in various combinations to protect the transmission of classified or unclassified-but-sensitive information:

(1) Encryption is a means for protecting information when it is transmitted over circuits vulnerable to interception or manipulation, as is the case with over-the-air transmission.

(2) There are a number of approved cryptographic products and associated keying materials that meet the requirement above listed in NSA's Information System Security Products and Services Catalogue or FIPS 140-1 Cryptographic Module Validation List and are either NSA or NIST certified.

(a) Type 1 products. Classified or controlled cryptographic item endorsed by NSA for securing classified and sensitive US Government information, when appropriately keyed.

(b) Type 2 products. Unclassified cryptographic equipment, assembly, or component, endorsed by the NSA, for use in national security systems as defined in Title 40, U.S.C., Section 1452.

(c) Type 3 Algorithm. Cryptographic algorithm registered by the National Institute of Standards and Technology (NIST) and published as a Federal Information Processing Standard (FIPS) for use in protecting unclassified sensitive information or commercial information.

(d) Type 4 Algorithm. Unclassified cryptographic algorithm that has been registered by NIST, but not published as an FIPS.

(3) There are instances where "double encryption" may be applied. Double encryption is the method used to separate traffic of different classifications requiring different encryption robustness sharing the same transmission system. Double encryption can be used to tunnel traffics of lower encryption robustness through circuits with higher encryption robustness, as well as the reverse.

b. The Use of Unencrypted Cable Circuits. Although encryption is the preferred protection, unencrypted cable circuits of copper or fiber-optics may be used. The degree of protection provided depends on the type of cable used. The least vulnerable to exploitation is fiber-optic cable, followed by copper coaxial cable and unshielded twisted pair

copper with solid and strand conductor options. Cable protection can be enhanced by burying the cable underground or in walls or floors and providing access controls for entry to cable vaults, rooms, and switching centers. Unencrypted cable circuits can be employed to transmit unclassified information under the following two conditions:

(1) When they are used only within the geographic boundaries of the United States or within areas totally within its control overseas.

(2) When adequate measures are implemented so that circuits are maintained on cable and not converted to unencrypted radio transmission.

c. All voice or data military radio systems used for transmitting classified or unclassified-but-sensitive information are secured or made securable by an approved cryptosystem. In the absence of embedded or machine cryptosystems for existing radio systems, operators will use auto-manual or manual cryptosystems to provide the needed security. Excluded from the foregoing cryptosystem requirements are the following:

(1) Radios that relay only encrypted information.

(2) Commercial systems purchased or obtained to fulfill an administrative function.

(3) Radios used for public safety communications with civil agencies or to communicate on civil aviation channels. This exclusion does not apply to communications dealing with aviation combat operations.

d. Appropriate physical, acoustical, electrical, or electromagnetic safeguards can protect communications circuits so that classified data can be transmitted on these lines in clear text. These circuits must be formally approved as a PDS as defined in reference i. A PDS is used only if it is cost effective and is sufficiently controlled to prevent covert penetration and interception. Systems that include a PDS to transmit data are not accredited to operate until the PDS is approved. Once a PDS is approved, no changes in installation, additions, or use may be made until the DAA or approval authority delegated by the DAA has granted approval for such changes.

e. Risk management practices are effected to determine and maintain the desired level of security throughout system employment.

3. Application of Risk-Management Techniques. The most effective protection for systems handling unclassified-but-sensitive information and first line of defense for any activity requiring protection is that accorded by the application of risk-management measures.

a. Overall Considerations

(1) Risk management is the process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. Network or circuit management authorities initiating risk-management action must identify the resources to be protected and analyze the risk of hacking, tampering, outright espionage, sabotage, damage, and theft to determine the minimum level of protection needed.

(2) Risk management offers a disciplined approach to identifying, measuring, and controlling certain events to minimize damage or loss to communication activities/systems. Its application can, at the same time, assist in optimizing the security return for each effort in which it is required. The objective of risk management is to achieve the most effective safeguards possible against deliberate or inadvertent:

- (a) Unauthorized disclosure of information.
- (b) Denial of service or use.
- (c) Unauthorized manipulation of information.
- (d) Unauthorized use.

b. Risk Assessments

(1) A risk is derived from the analysis of a threat and vulnerability. It serves as the core of the risk assessment, which requires a determination regarding relativity among risks and calculating associated damage or loss. This relativity forms the basis for effective countermeasures.

(2) A threat within the context of a risk analysis is any circumstance or event with the potential to cause harm to an information system in the form of disclosure, adverse modification of data, and/or denial of service. It can also be considered any agent/activity that could reduce or neutralize the effectiveness of a system, thereby limiting or negating mission accomplishment. Threat identification must account for both known and reliably postulated threats.

(3) A system vulnerability within the context of a risk analysis is a weakness in an information system or cryptographic system or its components (e.g., system security procedures, hardware design, internal controls, etc.) that could be exploited. It is often the totality of susceptibilities to specific threats but is, in itself, an absolute. The relationship between threats and vulnerability is considered in determining risk.

(4) Risk assessment in support of risk management is the process of analyzing threats to and vulnerabilities of an information system and the potential impact that the loss of information or capabilities of a system would have on force security or the effectiveness of a mission. Information that affects security must be developed using appropriate risk assessment methods. An analysis is thus required. The analysis is used as a basis for identifying appropriate and cost-effective countermeasures. It is likewise used to support the expenditure of resources and to determine the most cost-effective safeguards available.

(5) Commanders of deployed forces and activity managers determine relative risk. Risk is most accurately judged when specific vulnerabilities are matched to known threats. This type of assessment usually produces more reliable information with which risk may be described qualitatively. If no known threat exists, the vulnerability must still be evaluated for the potential opportunity it may offer a hostile element. Organization heads, in any case, must be prepared to react to the increased possibility of a threat. The risk-assessment process must automatically assume that hostile elements are prepared to take advantage of significant system vulnerabilities.

c. Management Decisions to Implement Countermeasures

(1) Reviewing identified risks and determining appropriate countermeasures is a function of commanders of deployed formations or activity managers, with advice from appropriate counterintelligence, physical security, and other functional area experts. Identifying areas of exceptional or unacceptable risk must be directly related to the organizational mission, goals, and objectives as stated by the commander or manager. At this point in the risk-management process, commanders can influence the commitment of resources and obtain the most effective return on investment. Analysis at this point may also reveal areas where reduced security may be appropriate, allowing for savings that can be applied in other operational areas.

(2) Selecting which security controls to implement must include a consideration of the possible degradation of operational efficiency. In many cases, security requirements will cause significant disruption of

managerial, operational, and administrative procedures and involve increased operating costs, which are all attributable to the requirements. Only a commander or designated accreditation authority (DAA) can properly judge acceptance and support the tolerance of such disruption relative to the increased security achieved. Such a condition requires that commanders and top-level management completely understand organizational dependence upon a system and its importance to mission accomplishment. A commander or DAA must resolve any perceived conflict between operational and security considerations

(3) If existing risks are unacceptable and the required security measures are deemed impractical or impossible to implement, the commander or DAA may opt not to operate in the environment available or terminate the operation of the system of concern.

4. Computer Security Measures

a. General Guidelines. DOD components deploying switched systems generally follow the guidelines laid down in reference d, amplifying Service regulations, and unified command directives in providing for the security of computer systems controlling their operating features or otherwise supporting their functions. Those computer systems are categorized as automated information systems (AIS) within the Department of Defense.

b. AIS Modes of Operation. AIS must be operated in accordance with prescribed processing modes. The security processing mode of an AIS is determined based on the classification or sensitivity and formal categories of data and the clearance, access approval, and need-to-know of the users of the system. Formal categories of data are those for which a written approval must be issued before access (for example, the compartments of Sensitive Compartmented Information (SCI), NATO information, or special access programs). The available or proposed security features of a system are not relevant in determining the actual security mode. All AIS will be accredited to operate in one of the following security processing modes:

(1) Dedicated Security Mode. A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data handled by the AIS.

(2) Systems High Security Mode. A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, but not necessarily a need-to-know for all data handled by

the AIS. If the AIS processes formal categories of information, all users must have formal access approval.

(3) Partitioned Security Mode. A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, but not necessarily formal access approval and need-to-know for all information handled by the AIS. When determining the security processing mode, one must consider only the classification and formal categories of data on the AIS and the clearance, authorization, and need-to-know of all users. If the system is properly sanitized between periods of processing, these factors may be considered independently for each period involved.

c. Minimum Requirements. IAW reference d, classified or unclassified-but-sensitive information will be safeguarded at all times while in AISs. Commanders and accreditation authorities may impose more stringent requirements based on their risk analysis. The requirements, in any case, provide for accountability, access control, training and awareness, physical controls, markings on output, "least privilege" measures (a person being provided entitled information, but no more), data continuity, data integrity, contingency planning, accreditation, risk management, and a life-cycle security plan. In addition to the foregoing requirements, AIS operating in other than the dedicated security mode must provide security features that meet the trusted system class in reference d as further guided by component Service instructions.

d. Software Controls

(1) Safeguards implemented for software will protect against compromise, subversion, or unauthorized manipulation.

(2) Only software that has been specifically developed or approved for use, or has been purchased or leased by an authorized Government representative, will be used with the AIS.

(3) Operational software will be modified and maintained only under rigorously controlled conditions requiring verification.

e. Hardware Security. Requirements for hardware as well as software security are equally significant considerations in providing for the security of switched-system AIS. Compensation must be considered in the absence of any resident security architecture, embedded security features, or hardware-based controls when providing for hardware security. Commanders and managers will, in any event, protect AIS

assets, whether hardware or software, under their control through cost-effective physical security measures.

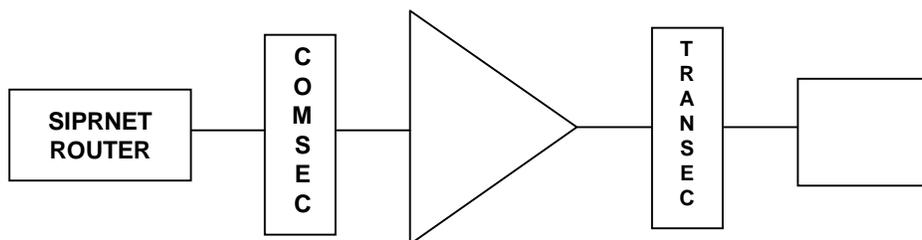
5. Recommended Security Measures for Switched-System Circuits

a. General Considerations

(1) COMSEC and TRANSEC devices are used to protect both classified and unclassified traffic passed via tactical switched systems within JTF networks. Their use applies to voice, data, and video information processing systems as well as to the associated communications interfacing equipment using varied transmission media. The services involved include those of the Defense Information System Network (DISN) common-user transports consisting of the Defense Switched Network (DSN), the Unclassified-but-Sensitive Internet Protocol Router Network (NIPRNET), and the Secret Internet Protocol Router Network (SIPRNET). Also involved are the services offered by other systems/networks including, but not limited to, those of the Joint World-Wide Intelligence Communications System (JWICS), the Defense Red Switch Network (DRSN), the Automatic Digital Network (AUTODIN)/Defense Message System (DMS), video teleconferencing (VTC), and telemedicine systems. They also include special-purpose and point-to-point circuits.

(2) With the application of any protection to switched-system circuits, special considerations must also be given to the type of transmission media used in connection with them. A radio frequency (RF)-type of medium such as satellite, tropospheric scatter, line-of-sight (LOS) radio, etc., or even laser radio, requires a stricter application of COMSEC and/or TRANSEC measures than metallic and fiber-optic cable transmission systems. The transmission media, thus, becomes the critical and primacy consideration when deciding on the application of COMSEC and TRANSEC devices. Also to be considered, as far as transmission is concerned, is the circuit type; i.e., whether it is a DOD-owned circuit, leased line, or commercial line (domestic or foreign).

(3) A COMSEC device mainly provides protection (encryption/decryption) for classified or unclassified operational information. A COMSEC device may also be used for other applications such as signal conversion (e.g., nonreturn-to-zero to conditioned diphase signaling) or with an unclassified system or circuit where a TRANSEC device is not used. A COMSEC device will normally receive clocking from a BLACK source except during an asynchronous mode of operation. See the illustration in Figure A-1.



MUX = MULTIPLEXER

MODEM = MODULATOR/DEMULATOR

Figure A-1. Typical COMSEC and TRANSEC Connectivity

(4) A TRANSEC device, as indicated above, provides for the protection of transmissions from interception and exploitation by means other than cryptanalysis and involves a number of measures to protect transmissions. They include such deterrent action as the application of low probability of intercept (LPI) techniques, frequency hopping, spread-spectrum transmission, the use of highly directional antennae, etc. A TRANSEC device likewise provides for traffic-flow security or so-called bulk encryption/decryption. This application is normally associated with a multiplexed interface or aggregate data prior to transmission or subsequent further multiplexing. A TRANSEC device can receive clocking from either a RED or BLACK source. The intent of a TRANSEC device is to randomize data flow so that there is no apparent change of activity on the circuit; i.e., it cannot be determined when a circuit is busy (in use) or not. Figure A-1 illustrates this condition as well.

(5) During deployments, authorities within joint forces must address additional considerations for overall information security within their organizations. Those include operations security (OPSEC) requirements that are based on a fundamental premise that military and government communications or information pertaining to military or government matters has an inherent OPSEC value, even if unclassified. The combination of unclassified information with essential elements of friendly information that may in itself be unclassified may become damaging when combined, or, in fact, become classified. These circumstances can include such matters as circuit activity, its detection, or its frequency of use (e.g., the number of times used per hour, the number of times used per day, etc.), which are examples of useful elements of information to an enemy. Increased traffic at a certain time by a support unit could be a tip-off for an enemy to seek out what is happening by tasking other intelligence-gathering resources. The

support unit may then be detected ordering rations, increased ammunition loads, or fuel by a certain day or hour, which would then signal an impending operation.

(6) Mobile Subscriber Equipment (MSE) operates within a secret-high network and uses a combination of COMSEC and TRANSEC devices to provide for protection with both encryption/decryption and traffic-flow security measures. However, because of the system architecture for MSE, a PDS must be established for the enclaves to operate within the network in a secret-high mode. Interoperability concerns must be considered when interfacing with TRI-TAC and other networks or systems that do not operate in a secret-high mode and a compatible encryption capability is unavailable. Another concern is the so-called "double encryption" requirement for SIPRNET traffic from an MSE element to a DISN standardized tactical entry point (STEP) site, a requirement established by the SIPRNET DAA.

b. Standing Rules

(1) All internodal operational and military official government information must be encrypted by channel or TRANSEC prior to RF transmission; e.g., via satellite links, LOS radio, etc., and provided information assurance IAW ref e.

(2) All intranodal operational military and official government information should be encrypted by channel or TRANSEC prior to RF transmission; e.g., LOS. However, special operational considerations may dictate exceptions to this rule. Who decides this exception, the deployed communications control center, senior communicator, system control duty officer, etc., should be clearly defined.

(3) Cable transmission systems can be employed in either a PDS or non-PDS environment. Cable transmission systems in a PDS environment do not require TRANSEC measures, and a COMSEC device is not required.

(4) The AN/FCC-100 and Integrated Digital Network Exchange (IDNX) do not have channel/port isolation. Terminating classified and unclassified circuits to these devices makes them RED, with appropriate care required.

(5) KY-68 and secure telephone units (STU)-III provide for end-to-end encryption, but do not provide a means to disguise circuit activity. The KY-68 and STU-III, moreover, also have a capability to operate in a nonsecure mode. The use of the KY-68 or STU-III in long-local or point-to-point applications using a first-level multiplexer, e.g., line termination

unit (LTU), remote multiplexer combiner (RMC), etc., requires the application of TRANSEC measures on the multiplexer composite.

(6) There is no need to encrypt individual unclassified circuits, e.g., NIPRNET, DSN, etc., if TRANSEC devices are used to cover the multiplexed output.

(7) Circuits traversing networks operating at secret-high that are interfacing to colorless or Black networks will require so-called "double encryption" even if the circuit is unclassified. The issue involved in this case is one of multiplexed data streams at different security classification levels passing over a single communications circuit. The intent behind "double encryption" here is to keep different classifications of information or data cryptographically separated when they share a transmission pipeline. So long as an approved device has encrypted each of the classified data streams, the resulting output is considered BLACK. Unlike other references to double encryption in this discussion, i.e., where double encryption refers to the use of both information/data encryption and TRANSEC encryption used as shown in Figure A-1, the situation described here is more representative of actual double data encryption, where encryption is used to separate different levels of traffic regardless of whether or not TRANSEC encryption is used.

c. Prescribed Supplementary Rules

(1) DSN traffic is essentially unclassified or BLACK information because the DSN is intended to be used for the transmission of only unclassified or encrypted (e.g., STU-III) information. DSN traffic thus requires a minimum of bulk encryption or a TRANSEC device prior to internodal RF transmission.

(2) The NIPRNET likewise, because of its unclassified nature, requires a minimum of bulk encryption or a TRANSEC device prior to RF transmission. The foregoing standing rules and subparagraph (1) above reflect the requirement for data encryption before RF transmission, additional TRANSEC encryption notwithstanding.

(3) SIPRNET traffic is classified or RED information because the SIPRNET is intended to be used for the transmission of classified information up to the secret level. It requires a COMSEC device prior to RF transmission.

(4) Joint Worldwide Intelligence Communications System (JWICS) is protected in similar fashion as the SIPRNET. However, the COMSEC devices protecting JWICS must be keyed at the highest level of the traffic to

be protected. For JWICS, this keying is for traffic above the secret level.

(5) TRANSEC is appropriate for VTC circuits regardless of whether or not any are protected further with COMSEC based on the classification level of the traffic.

(6) As far as AUTODIN is concerned, the circuits handle both classified GENSER and Defense Special Security Communications System (SCI) traffic and require both COMSEC and TRANSEC protection. As far as upcoming DMS circuits are concerned, they can be classmarked to carry traffic from the "unclassified" to "top secret" level. Transmissions must be protected up to the highest level the system is classmarked to process. They require COMSEC measures prior to transmission.

d. Configuration Examples

(1) Figures A-2 through A-9 are examples of tactical security configurations for the transmission of information processed through switched systems.

(2) Figure A-2 is an example of a valid configuration where both COMSEC and TRANSEC devices are used.

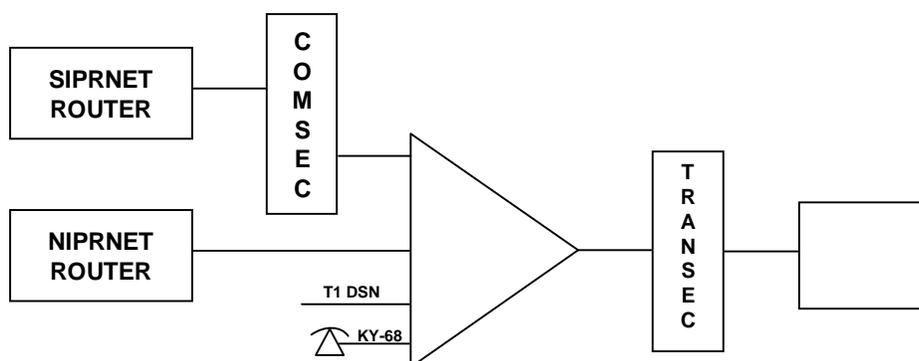


Figure A-2. Valid Internodal Configuration

(3) Figure A-3 is an invalid configuration because there is no TRANSEC device to cover the activity or information on the DSN or KY-68 interfaces.

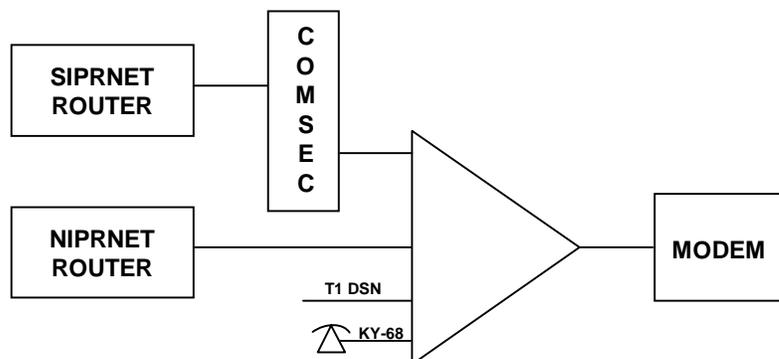


Figure A-3. Invalid Internodal Configuration

(4) Figure A-4 is also an invalid configuration because there is no means to disguise the activity of traffic with the KY-68s or preclude its transmission in a nonsecure mode. However, Figure A-4 may be valid if TRANSEC, in particular traffic-flow security, is not a concern in the deployed environment. Since, in such a case, the minimum requirement of all traffic encryption is being met, the validity of the configuration is a function of risk assessment.

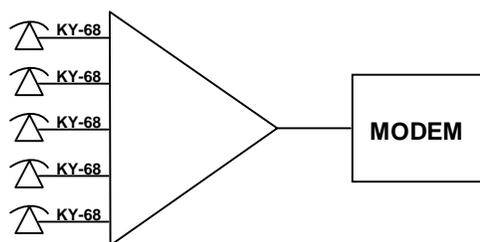


Figure A-4. Invalid Internodal Configuration when TRANSEC is of Concern

(5) Figure A-5 is a valid configuration. The activity and information of the circuit is disguised by use of a COMSEC device. However, the configuration may not be valid if the risk assessment determines that the operating environment requires TRANSEC.

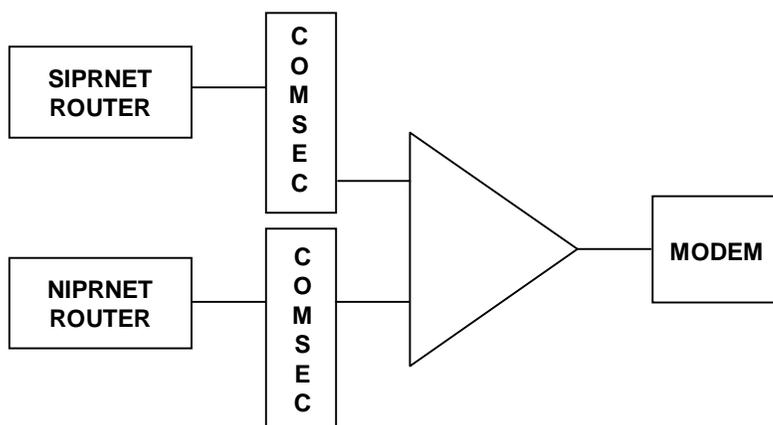


Figure A-5. Valid Internodal Configuration When TRANSEC is Not of Concern

(6) Figure A-6 shows an application where a COMSEC device is used for signal conversion. This configuration could also be used when going between networks operating at one security level through networks operating at different security levels using tunneling techniques.

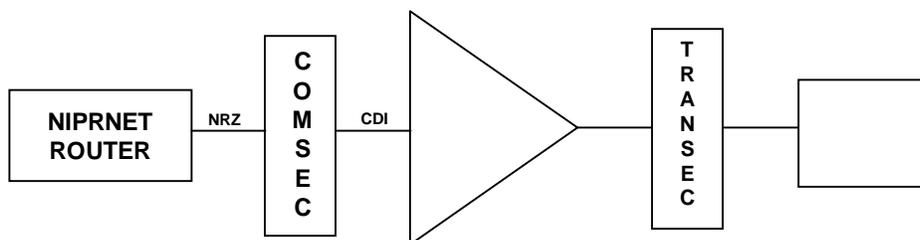
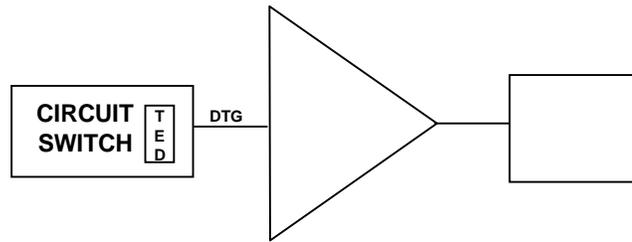


Figure A-6. Valid Internodal Configuration

(7) Figures A-7, -8, and -9 depict circuit switch configurations, both valid and invalid. If a PDS-Yes (MSE switch) Digital Trunk Group (DTG) as in Figure 9 is RED, the MUX in this configuration would also be RED.



DTG = DIGITAL TRUNK GROUP
TED = TRUNK ENCRYPTION DEVICE

Figure A-7. Valid Internodal Configuration

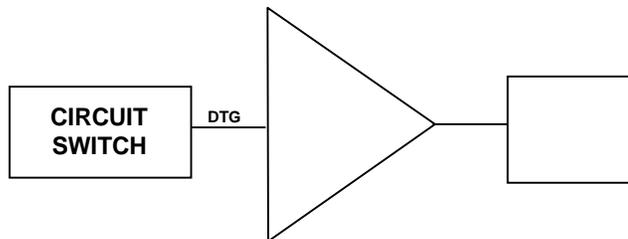
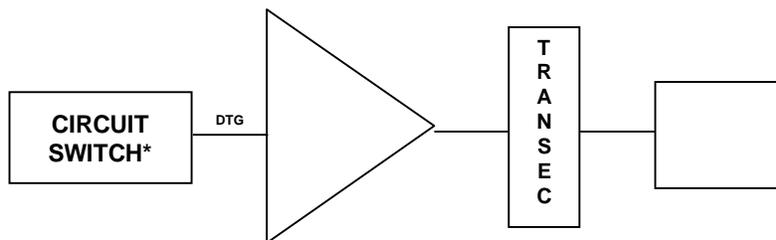


Figure A-8. An Invalid Internodal Configuration



* Applies only to PDS-No switches

Figure A-9. Valid Internodal Configuration

e. TEMPEST Guidance for Clocking Key Generator (KG) Installations.

(1) Answers to the four questions listed below may provide guidance for TEMPEST requirements concerning KG installations. The answers do not provide a person with strict rules, but serve as guidelines that apply in most cases. If there is any doubt, one's certified TEMPEST technical authority (CTTA) should be contacted. These guidelines apply not only to KG-84s, but also to trunk encryption devices.

- (a) Is the KG used only for TRANSEC?
- (b) Is the KG-encrypted output routed to a modem?
- (c) Does the source of the KG clock process classified data?
- (d) Is the signal input to the KG classified?

(2) Guidance based on answers to the preceding questions is as follows:

(a) If the answer to subparagraph (a), above, is yes, there is no RED/BLACK installation requirement.

(b) If the answer to (b), above, is yes, (c) is no, and (d) is either, there is no RED/BLACK clocking restrictions.

(c) If the answer to (b) is yes, (c) is yes, and (d) is yes, there is no RED/BLACK clocking restrictions.

(d) If the answer to (b) is no, (c) is yes, and (d) is either, consult your CTTA.

ENCLOSURE B

RESPONSIBILITIES

1. Joint Staff. The Director for C4 Systems, Joint Staff (J-6), is assigned primary responsibility for direction and guidance regarding the interoperability of deployable switched systems in support JTFs, to include the security of the communications traffic that flows through them. The J-6 is also responsible for:

a. Conveying and coordinating joint communications guidance and direction among the DOD components.

b. Furnishing advice and assistance for communications matters, as required, to the joint switching community.

c. Serving as the primary Joint Staff authority for the establishment of joint communications doctrine and for the employment of communication systems in support of deployed joint forces.

d. Advising the strategic, as well as tactical switching community on joint tactical matters and employment concepts in order to provide for the vertical and lateral interoperability of DOD-component communication systems during joint operations.

e. Establishing basic security guidelines and providing guidance for switched-system security to ensure switched-system interoperability while operating within security envelopes.

f. Monitoring the needs of joint commands with regard to switched-system support and keeping abreast of related developments within the joint switching community to ensure that switching requisites in support of deployment requirements, to include those dealing with security, are fulfilled.

g. Directing and guiding the efforts of the EA-TJTN in coordinating the activities of the joint switching community in order to provide for the secure interoperability of tactical switched systems.

h. Participating in the activities of the Theater Joint Tactical Networks Configuration Control Board (TJTNCCB) to resolve technical interoperability issues with regard to tactical switched systems and deployable networks.

i. Convening the Military Communications-Electronics Board or directing meetings of its panels to resolve tactical switching issues, to include related security issues.

j. Mediating in disputes concerning connectivity between and among different systems and networks when beyond the capabilities of the activities mentioned in paragraph 2 below to resolve.

2. Military Services, Defense Agencies, Combatant Commands, and deployed JTF's/JSOTF'S and their components

a. Apply the security measures defined in references a through i on a day-to-day operational basis.

b. Implement the rules outlined in this instruction by ensuring that subordinate elements likely to deploy or to participate in joint operations apply the rules as required.

c. Conduct risk assessments and apply the risk management procedures addressed in this instruction.

d. Ensure that switching equipment acquired for use by deploying forces has the capability of implementing the measures defined in this instruction.

e. Participate in the proceedings of the TJTNCCB that address the rules in this instruction or similar stipulations and recommend updates as required.

f. Resolve disputes concerning connectivity between and among different systems and networks with the appropriate combatant command, acting as the mediator and applying the advice of the NSA, Joint Interoperability and Engineering Organization, and JCSE.

3. Defense Information Systems Agency (DISA). In addition to applicable responsibilities defined in paragraph 2 above, DISA:

a. Manages the Defense Information Infrastructure (DII), to include the Defense Information System Network (DISN) and related networks and systems, and provides for its security as required.

b. Provides advice and assistance on securely interfacing tactical switched systems with those of the strategic communications community.

c. Provides system interoperability certification and interfacing test support through the Joint Interoperability Test Command.

d. Serves as the DOD switched-system integration manager and works with the EA-TJTN in overseeing and coordinating tactical switched system acquisition, development, modification, and employment.

4. National Security Agency and Defense Intelligence Agency (DIA)

a. Provide advice and assistance to the joint switching community as required, regarding tactical switched-system security.

b. Assist operational commands with risk assessments as required.

c. Participate in the proceedings of the TJTNCCB and provide advice and assistance on the development of security guidelines for tactical switching operations.

5. Defense Intelligence Agency

a. Manages the operation and security of the JWICS wide-area intelligence network.

b. Participates in the proceedings of the TJTNCCB and provides advice on issues regarding the JWICS, TROJAN SPIRIT, and other communications systems supporting intelligence operations in deployment zones.

6. US Army Program Executive Officer for C3 Systems as the DOD EA-TJTN IAW reference g

a. Coordinates the efforts of the joint switching community in providing for the secure interoperability of tactical switched systems.

b. Coordinates efforts within the joint switching community to maintain configuration control over deployable switched-system applications, components, and networks, to include the implementation of security measures.

c. Initiates and coordinates tests and user exercises to evaluate switched-system and network configurations, assess the introduction of new technology and concepts, and resolve interoperability issues, to include those involving security.

d. Coordinates as required with DISA to ensure that deployable switched systems can be effectively and securely interfaced with the DISN and other strategic networks serving as part of the DII.

e. Convenes the TJTNCB to resolve tactical switched-system interoperability issues, to include those that affect the security of JTF networks.

ENCLOSURE C

REFERENCES

- a. DOD Directive 5200.1, 13 December 1996, "DoD Information Security Program"
- b. DOD Regulation 5200.1-R, 17 January 1997, "Information Security Program Regulation"
- c. DOD Directive - C - 5200.5, 21 April 1990, "Communications Security" (U)
- d. DOD Directive 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems"
- e. CJCSI 6510.01B, 22 August 1997, "Defense Information Operations Implementation"
- f. DOD Instruction 5200.40, 30 December 1997, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"
- g. Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) memorandum, 27 September 1999, "Theater Joint Tactical Networks (TJTN) -- Executive Agent Assignment"
- h. DOD Chief Information Officer Guidance and Policy Memorandum No. 6-8510, 16 June 2000, DoD Global Information Grid Information Assurance,
- i. NSTISSI 7003, 13 December 1996, "Protected Distribution Systems"

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATION AND ACRONYMS

AIS	automated information standard
AUTODIN	Automatic Digital Network
CIO	Chief Information Officer
COMSEC	communications security
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Accreditation Authority
DII	Defense Information Infrastructure
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DOD	Department of Defense
DMS	Defense Message System
DSN	Defense Switched Network
DTG	Digital Trunk Group
EA-TJTN	Executive Agent for Theater Joint Tactical Networks
EUCI	endorsed for unclassified cryptographic item
FIPS	Federal Information Processing Standard
G&PM	Guidance and Policy Memorandum
GENSER	General Service
IDNX	Integrated Digital Network Exchange
INFOSEC	information security
JCSE	Joint Communications Support Element
JTF	joint task force
JWICS System	Joint World-Wide Intelligence Communications
KG	key generator
LOS	line of sight
LPI	low probability of intercept

LTU	line termination unit
MSE	mobile subscriber equipment
NATO	North Atlantic Treaty Organization
NIPRNET Network	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OPSEC	operations security
PDS	protected distributed system
RF	radio frequency
RMC	remote multiplexer combiner
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
STEP	standardized tactical entry point
STU	secure telephone unit
TJTN	Theater Joint Tactical Network
TJTNCB	Theater Joint Tactical Network Configuration Board
TRANSEC	transmission security
VTC	video teleconferencing

PART II -- DEFINITIONS

classified information. Official information regarding the national security that has been designated "TOP SECRET," "SECRET," or "CONFIDENTIAL" according to Executive Order 12356.

communications security (COMSEC). Protective measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emissions security, and the physical security of COMSEC material.

COMSEC device. Equipment designated to provide security for telecommunications by converting information to a form unintelligible to an unauthorized interceptor and, subsequently, by reconverting such information in its original form for authorized recipients. Also, equipment designed specifically to aid in, or as an essential element of, the conversion process.

NOTE: COMSEC equipment includes cryptoequipment, cryptoancillary equipment, cryptoproduction equipment, and authentication equipment.

COMSEC threat assessment. Actions taken to determine the technical and operational capability of a hostile entity to detect, exploit, impair or subvert friendly telecommunications. COMSEC threat assessment is also action taken to determine the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Cryptosystem. The associated items of COMSEC material used as a unit to provide a single means of encryption or decryption.

information security. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and the denial of service to unauthorized users.

protected distribution system (PDS). A wireline or fiber-optics system that includes adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for unencrypted transmission of classified information.

risk

a. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the damage severity that the resulting adverse impact will represent. Risk is essentially the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood of a threat occurrence resulting in an adverse impact (e.g., denial of service) with the severity of the resulting adverse impact. Reducing the threat or the vulnerability reduces the risk.

b. The possibility that a particular threat will exploit a particular vulnerability of a system.

risk assessment. The process of analyzing threats to and vulnerabilities of an information system and the potential impact of the loss of information or the capabilities of a system would have on national security. The process includes using the resulting analysis as a basis for identifying appropriate and cost-effective countermeasures.

risk management. The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

switched system. A telecommunications system that receives and routes communications traffic within the circuits of a switched network until it reaches its destination at a subscriber terminal and establishes end-to-end communications connectivity between two or more subscribers.

telecommunications. The transmission, communication, or processing of information, including the preparation of this information by electrical, electromagnetic, electromechanical, or electro-optical means.

telecommunications system. Any system that transmits, receives, or otherwise communicates information by electrical, electromagnetic, electro-mechanical, or electro-optical means. A telecommunications system may include features normally associated with computers.

threat. Any capability, circumstance, or event with the potential to cause harm to an information system in the form of destruction, unauthorized disclosure, adverse modification of data, and/or denial of service.

transmission security (TRANSEC). The component of COMSEC that results from the application of measures designed to protect

transmissions from interception and exploitation by means other than cryptoanalysis.

TRANSEC device. Equipment designed to protect telecommunications transmissions from interception, exploitation, or disruption by means other than cryptoanalysis. It may provide for traffic flow analysis with encryption, but can provide for antijamming protection.

Unclassified-but-sensitive information. Any unclassified information, the loss, misuse, or unauthorized access or modification of which could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under the Privacy Act.

vulnerability. A weakness in an information or cryptographic system or its components (e.g., system security procedures, hardware design, internal controls, etc.) that could be exploited.

(INTENTIONALLY BLANK)