Appendix 6: Joint IA Policy

1. Purpose

The purpose of this appendix is to promulgate general Information Assurance (IA) guidance to headquarters elements of current and potential users of the Joint Mobile Network Operations (JMNO) TTP. Requirements for IA or Information Security (InfoSec), in the context of Information Operations (IO), are provided herein to ensure a continued high level of systems confidentiality, integrity, and availability of information products.

Proper security of Automated Information Systems (AIS) and data is an important integral part of the overall network security posture. AIS technology provides powerful work tools and users have expansive access to information. Information processing and distribution can be accomplished quickly and easily, but AIS technology also presents serious risks to the information it supports. If not addressed, these risks can result in operational disruptions, compromise of classified or otherwise sensitive information, and/or serious mission degradation. Commanders shall ensure continual and full compliance with the Information Systems Security and Information Assurance (IA) requirements outlined in this appendix.

Information Systems Security is dependent on the individual user. Disciplined use is critical to both individual workstations and system or network security. The quantity of data that can be stored on removable media necessitates strict user controls, to include proper labeling and handling. Poor user discipline can introduce crippling computer viruses or other malicious software code sequences or provide openings for hostile penetration of computer networks, with impacts far beyond the local level.

2. General

IA activities here-in focus on providing information assurance to subscribers of the network. IA relies on four inter-related processes. These include a process to protect information and information systems, a process to detect attacks or intrusions, a restoration process to mitigate the effects of incidents and restore services, and a response process. IA strives to constantly improve the security posture of the Command's information infrastructure.

3. Policy

a. <u>AIS Security Training and Indoctrination</u>

IA/InfoSec training is a fundamental requirement. A valid IA/InfoSec program requires that all personnel performing AIS user, management, administration, or security functions are knowledgeable of requirements. The CJCSM 6510.01_ requires all users of DOD IAS to complete IA training. All deployed users of NETWORK information systems shall complete an AIS security indoctrination course prior to receipt of a user identification (USERID) and password for access to any Government network. Commanders will ensure that user awareness training is conducted at least annually to comprise training including but not

limited to: robust password/pass-phrase development, password protection, e-mail security, shoulder-surfing, workstation terminal locking, anti-virus procedures, incident reporting procedures, AIS-related Operational Security (OPSEC), and any pertinent Service policies. Upon user indoctrination at his/her work area, the Terminal Area Security Officer (TASO) will brief the user on the local AIS security requirements.

b. AIS Accreditation

The appropriate Designated Approving Authority (DAA) must accredit TOP SECRET, SECRET, CONFIDENTIAL, CLASSIFIED RELEASABLE, and UNCLASSIFIED, AIS prior to operation or connection to a network. In accordance with the CJCSM 6510.01_, "The DAA will be an employee of the US Government (USG) (minimum grade of O-6/GS-15), will comply with the security requirements of DOD 5200.2-R" and "….hold USG security clearance (such as, TOP SECRET) and access approvals commensurate with all information systems under the DAA's jurisdiction." Any changes to the AIS, level of data processed, operating systems or associated environments that affect the accredited safeguards or security requirements will require an update/re-accreditation. The DAA should be technically competent, with the authority to procure required countermeasures to ensure an acceptable level of processing risk and the authority, if necessary, to shut down computer or network operations.

c. AIS Systems and Network Connections

(1) Interconnection of new systems requires accreditation in accordance with the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and as outlined in Tab N of this appendix, in accordance with reference (f) and/or subsequent regulations.

(2) Connection to SIPRNET/NIPRNET Integrated Tactical Strategic Data Network (ITSDN) gateway routers will not be activated or installed until a copy of all accreditation documentation, signed by the organizational DAA for Secret and below, is furnished and accepted by the Defense Information Systems Agency (DISA). In support of this effort, both SIPRNET and NIPRNET Connection Approval Process (CAP) documentation is required. The Department of Defense (DOD) SIPRNET and NIPRNET Program Manager is the collection point for all CAP documentation. Information and procedures for completing CAP documentation may be found at https://iase.disa.mil/. JTF and Service Component DAAs are responsible for obtaining like assurances from lower-echelon router owners prior to allowing further interconnection. Accreditation guidance is contained in Tab N of this appendix.

d. AIS Security Inspections

A program for conducting annual reviews of the adequacy of the safeguards for operational, accredited AIS should be established. Tab O of this appendix identifies preparation procedures and timeframes for IA inspection of Component Commands.

e. Basic Installation/Operating Requirements

Networks, access points to the Defense Information System Network (DISN), AIS computer hardware and software that comprise them are Government property intended specifically for official use. The Government reserves the rights to access, review, copy, delete, disclose, retrieve and/or monitor any and all information transmitted or stored within these assets for any appropriate business purpose. The content or access to electronic information is not private, and DOD employees and contractors shall have no expectations of privacy. The ease and convenience with which information can be transmitted and/or stored by use of computer assets require that all users unfailingly apply the following rules to govern their system use:

(1) Compose all electronic communications with the same degree of care and discretion as you use for official correspondence. Write messages in courteous, professional, and businesslike terms and do not forward obscene or otherwise potentially offensive material.

(2) Take care to preserve the confidentiality of data on the AIS by rigorously restricting system access and protecting passwords and USERIDs.

(3) Personnel shall not use the Government AIS assets for significant personal use. Your use of these assets is governed by the same rule that applies to use of Government telephones: Government systems are intended for business use and are available only for limited personal use that does not interfere with performance of job functions and organizational mission, and is conducted in a professional manner.

(4) Terminal Area Security for AIS Processing Classified Information.

(a) Terminals processing classified data must have the transmission protected through a NSA Type I encryption, or an approved Protected Distribution System (PDS).

(b) A classified terminal must be in an approved open storage area, under constant observation of cleared personnel, or all classified media must be stored in a safe.

(c) A classified terminal may be located in a normal office environment provided:

1 All storage is removable and stored in an approved container. All memory is volatile and powered off when classified processing is complete.

2 Communications are severed at the host when classified processing is completed.

3 The area is protected from observation by non-cleared personnel during classified processing.

4 The area must be secured by at least a key lock when not occupied.

(5) Terminal area security for AIS processing unclassified information must allow for protection against unauthorized access and theft. The terminal must be password protected and never left in a logged-on configuration

(6) AIS monitors and printers must be positioned to restrict viewing of data to individuals cleared for and authorized access to the information. In mixed environments such as those with coalition partners where SIPRNET and Combined Enterprise Regional Information Exchange System (CENTRIXS) are both in use or where coalition partners routinely have physical access, SIPRNET terminals must be positioned so that coalition members cannot view the screen. Utilize privacy screens on SIPRNET monitors where positioning is not practical or to enhance protective measures.

(7) AIS must be physically controlled while processing classified information.

(8) Operating System screen saver password locks shall be active at all times and will not exceed 15 minutes activation delay.

(9) Each DOD AIS, network or stand-alone, shall display a DOD approved warning banner at the time of LOGON, such as the following extracted from reference (l).

> THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED US GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED.
>
> USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.
>
> (A separate warning screen for CENTRIXS is provided in Tab J to this appendix.)

f. Personnel Security

All personnel with unescorted access to areas containing AISs must be cleared for the highest classification level being processed or openly stored in the area and have the appropriate need-to-know.

g. Hardware Security

(1) AISs and associated equipment must be protected at the highest level of classification of information on the system.

(2) Classified equipment will not be removed from authorized work areas (such as, sent to vendor for repair) without the approval of the TASO. All classified information must be removed and internal Information Storage Media (ISM) degaussed and declassified in accordance with procedures outlined in paragraph 3.q.

(3) Prior to deploying an AIS workstation which has been used for classified processing or which will be connected to a classified network, the responsible TASO will identify a person responsible for providing AIS security in transit. This individual will obtain permission to transport materials in accordance with local procedures. Upon arrival at the deployed location, this individual will be responsible for the security of the equipment until it has been formally delivered and accepted by the user.

(4) System administrators will disable built-in peripherals (modems, microphones, Infrared (IR), serial, parallel, firewire, Universal Serial Bus (USB), video, etc.) that are not in accordance with the network accreditation. Modems will never be active while the system is connected to the network. Procurements of computer equipment should specify the ability to disable built-in peripherals whenever possible. The use of full motion cameras connected to AISs will not be permitted without the express permission of the local DAA in writing due to the increased security risk and high bandwidth usage.

(5) All unused Input/Output (I/O) ports like serial, firewire and especially USB ports should be disabled on systems where they are not needed. As additional security, software should be used that restricts the use of authorized peripheral ports to specific device types to prevent an authorized device from being disconnected and an unauthorized device being used.

(6) Non-DOD devices shall not be used to access DOD networks unless the local DAA has granted written authority for the specific device to access the unclassified network. Local system administrators will ensure the computer complies with the security requirements enforced on like government devices and the drives are loaded with Government software load-set. Prior to return to the user, the non-DOD device must not contain any classified material and the Government load-set must be wiped from the device. Personally-owned Palm-top computers not capable of the same security provided by standard network workstation Windows operating systems (such as, Windows 2000) are excluded from access to Government networks regardless of load-set. Non-DOD devices will not be connected to a classified network.

h. Software and Information Storage Security

(1) ISM will be marked and safeguarded in accordance with the highest classification of information processed on the AIS in which the ISM has been used. Removable media and peripheral components, with a storage capability, inserted or utilized in an AIS that processes classified information will be classified at the highest level of information that the AIS processes and must be appropriately labeled and protected. Newer technologies that act as removable secondary storage media will be handled in the same manner. For the purposes of this instruction, newer technologies such as Digital Media, Flash Media, and Optical recorders are included in the ISM definition.

(a) Removable and peripheral digital media storage devices or storage media that are too small for the normal GSA Standard Form sticker to be attached will have the appropriate classification marked directly on them using a permanent marker and have a tag attached that clearly designates the media classification. Devices shall have the capability to enforce file security objectives imposed by an operating system. Devices shall have a physical write protect mechanism. Digital storage media shall be "domain specific" and are NOT authorized to be introduced to multiple AISs of differing classification levels. In accordance with DISA guidelines, DOD computing assets shall have the capabilities to enforce discretionary access control measures (file/object/user) found in existing, certified operating systems (OS). These capabilities shall be actively used.

(b) It is essential in the procurement of storage media that unit commanders establish common device standards as well as limit the use (quantity) of such devices. A robust media asset issue and control program is central to this issue. Procurement of digital storage device(s) that provide inherent protected file access, physical write protection and/or imbedded biometric device access control are minimum guidelines to assist the procurement process.

(c) In all respects, data of all formats stored on such a device will be afforded commensurate physical protection in the storage, use, transmission (conveyance) and destruction of the device continuously and throughout its lifecycle.

(d) Government storage media shall be exclusively used in Government computing devices. Use of non-DOD removable storage media accessing Government computer devices is not authorized. Contractor-procured storage is authorized if procured in direct support of the contract.

(2) Prior to loading any data files from sources external to the device, the data will be scanned for viruses.

(3) Commanders will ensure that servers and workstations, whether connected to enclave networks or stand-alone, are updated with the latest anti-virus software and signature files on a frequent and scheduled basis.

(4) Software license and copyright requirements shall be adhered to at all times.

(5) Joint Task Forces (JTF) and Service Components will develop baseline software installations for all their AISs. Methods must be in place to ensure that the baseline is tested and updated as new patches and security settings are required. Use of the DISA Gold and Platinum disks as the starting basis for all baseline installations is recommended.

i. Security Patch Management

(1) There are many automated patch management solutions available that provide options for deploying security patches to network computer systems. The goals of security patch management are to:

- Provide a method for testing security patches prior to installation to ensure continued system availability to meet operational requirements
- Provide for proactive implementation of security patches to keep systems secure and reliable
- Provide access to systems on the network to measure the effectiveness of security patch management

(2) Units will develop, document, and employ procedures to accomplish the task of implementing security patches. Many units utilize a baseline system load (or image) to create new client systems. One of the frequently overlooked actions in the patch management process is updating the system baseline. Keeping the system baseline current eliminates the need to update systems once they are fielded.

j. Palm-Top Computer Security

Palm-top personal digital assistants (PDA) or handheld computers present significant security risks to DOD-Interest computer networks and information. The risks could outweigh the convenience value the devices provide. The threats include: minimal operating system security features, no file/data security, act as a source for spreading malicious code (such as, viruses), potential of theft and loss or compromise of information. These risks force the following policies:

(1) Radio-Frequency-Capable wireless palmtop computers/PDAs may not be used except by written permission from the cognizant Combatant Commander J6. Any procurement requests for such devices must be vetted through unit System Security Officer and TASO for acceptance prior to purchase. Additional guidance on wireless technology can be found in Tab M of this annex.

(2) Palmtop computers/PDAs shall not be connected to classified AISs. Classified material or overtly sensitive information, such as flag officer travel schedules, account passwords, may not be introduced to these systems at any time.

(3) Government palmtop computers/PDAs **may** be synchronized to Government unclassified (such as, NIPRNET-connected) workstations. Use of unauthorized freeware or shareware on these Government devices is prohibited and anti-virus software must be installed and enabled.

(4) Synchronizing or otherwise connecting non-DOD palmtop computers/PDAs to any Government computer or network is prohibited, except as defined previously in paragraph 3.g.(6).

k. Local Area Network (LAN) Security

(1) All network systems must be able to identify users by means of a USERID and then authenticate by use of a password (See Tab D). USERIDs and passwords are the unique identifiers of an individual authorized access to a network system and shall not be divulged to anyone. Network systems shall be configured to audit actions taken by each individual.

(2) The entire LAN and all equipment connected to it must be protected at the highest classification level of information processed on the LAN.

(3) Files that have restricted need-to-know information require additional safeguards from general access (such as file/directory permissions and/or passwords).

(4) Local Area Networks use communications components and data cabling (such as, fiber, twisted pair) to interconnect network components. Connectivity to communication components, for fixed classified LANs, outside controlled areas must be protected in accordance with reference (p). Cabling shall be separated as prescribed in NSTISSAM TEMPEST 2-95, section 3. Whenever possible, shielded twisted pair or fiber optic will be used for data cabling. Fiber cabling shall be marked at each end to indicate the network it supports. To ensure easy identification of classified and non-classified data cabling the following cabling color scheme will be used.

(a) Yellow (or Orange if XNET is not used) – Top Secret

(b) Red - SIPRNET

(c) Green (preferred) or Black or White or Gray–NIPRNET

(d) Blue – Global Counter-Terrorism Force (GCTF) -0

(e) Blue/White – Global Counter-Terrorism Force (GCTF) -1

(f) Orange – XNET

(g) Brown – Multinational Coalition Forces Iraq (MCFI)

(h) Purple plus second color – Bi-Lateral Networks

(5) When network resources (such as, shared directories) or functions (such as, user authentication) must traverse the DISN a separate, encrypted sleeve (for example, IPSec, VPN) will be used to connect the networks.

(6) Individual accountability on the LAN will be enforced. Authorized network users will be provided an individual account when they have received proper training and signed a user agreement form. System administrators will not share a common user account to administer the systems on the LAN. System administration accounts must remain uniquely identifiable to a specific individual to ensure accountability. Positional accounts may be used when: a) they are tied to and signed for by a single responsible individual or b) for watch-officers, such accounts will be limited to a specific machine for duty requirements and watch-officers will sign agreements that indicate that they are responsible for the account during their shift. Written (paper or electronic) logs shall be maintained to indicate the date and time a watch officer takes charge of a particular watch-standing account.

l. Transmission Security

Transfer of data over telephone lines requires extra precautions and specific procedures to preclude inadvertent transfer or compromise of classified data. Requests to connect Secure Telephone Equipment (STE) or modems to computers, facsimile machines, etc., will be forwarded to the appropriate DAA for approval.

m. Emanation Security

All AIS equipment will be installed in accordance with national TEMPEST standards. Red/Black separation criteria must be maintained at user workstations and for cabling as noted in paragraph 3.k.(4).

n. AIS-Produced Documents

Security requirements for AIS-produced documents (complete, partial, or draft "working papers") are the same as for documents produced by any other means. DOD 5200-R and 5200.1-PH provides expanded requirements.

(1) AIS output products must be controlled, stored, transferred, marked, accounted for, classified, declassified, and downgraded consistent with the highest classification of information contained within, or the overall classification of the complete product, whichever is higher.

(2) Printouts will be reviewed for classification and content, properly marked, and controlled in accordance with DOD Information Security requirements.

o. Transferring Files From Classified AIS

Frequently, there is a need to transfer data between AISs of differing classifications. Since data residing on a system is classified at the highest level of any information contained on the AIS, extraction of data must be done carefully to protect against inadvertent transfer and possible compromise of classified information. If the classification level of the AIS is

TS/SCI, the user must follow the procedures set by the Command's Special Security Office (SSO).

p. Transferring Files To Classified AIS

Transferring unclassified files to a classified computer system may be done using removable media once you scan the disk for viruses while still in the source system and enable physical write-protection on the removable media. Placing removable media without a physical write-protection capability into a system with a higher classification results in a change of security classification of the media to the highest level processed on the destination system. The final action is to scan the media on the destination system for viruses.

q. Declassification of ISM

(1) ISM will be safeguarded based on the highest classification of information ever processed on the AIS until the ISM is declassified or destroyed.

(2) ISM used in classified systems shall not be declassified or released from control without the approval of the cognizant TASO. TS/SCI ISM must be declassified in accordance with Service Component SSO procedures.

(3) There are currently no NSA-approved disk-wipe utilities to declassify a magnetic hard drive for reuse in a system at a lower classification. Once available, NSA-approved utilities may be used by TASOs to erase data from ISM classified SECRET and below (except optical ISM). TASOs must ensure these utilities are used properly and the downgrade form is completed with all pertinent information. Each action taken to clear or declassify ISM should be verified to ensure classified information located on the media was destroyed correctly.

(4) All ISMs identified for destruction must be declassified by a Government-approved degausser or disk shredder, or complete sanding of each of the magnetic surfaces. The degausser will be certified to a level equal to or higher than the maximum coercivity, which is the intensity of the magnetic field needed to reduce the magnetization of a ferromagnetic material to zero after use, (measured in oersted) of the media. Media that exceeds the maximum oersted rating of the degausser must be physically destroyed.

(5) Optical ISM can only be declassified by total destruction (such as, incineration or shredding in an optical media approved shredder).

(6) Declassifying a disk requires proper documentation.

r. Foreign National Network Access

(1) DOD personnel may operate computer systems registered within the .mil domain. Procedures for Foreign Nationals to gain access to the Internet via limited NIPRNET services are outlined in Tab I.

(2) The SIPRNET is a US only network regardless of data releasability. Classified processing by Foreign Nationals shall be conducted on Coalition networks approved for such use. Tabs J and K provide additional details and policy for CENTRIXS networks.

s. Voice Over Secure Internet Protocol (VoSIP)

Voice over IP (VoIP) technology has become commonplace commercially in the past few years. This technology has been successfully implemented over classified and unclassified military networks. When VoIP is implemented on the SIPRNET it is referred to as Voice over Secure IP (VoSIP). Users shall protect the enabled (user logged in) VoSIP phone commensurate with the classification of the network to which it is attached. Users shall keep the enabled phone under the operational control of at least one appropriately cleared, authorized person when personnel not cleared to the level of the attached network are in the area. The user shall disable (log out) the phone when authorized personnel leave for the day or otherwise leave the area unattended, unless the phone is in an area approved for open storage of classified material at the security level of the network to which the phone is attached.

4. Execution

a. Concept of Operations

(1) General. The Theater Computer Emergency Response Team (CERT) and Theater Communications Control Center (TCCC) IA organization are key parties with respect to the IA posture. Together they provide a multi-tiered IA response capability for deployed commands and users of NETWORKaccess systems. The mission of the CERT and TCCC IA is to defend NETWORKsystems' availability, integrity, and confidentiality through the execution of IA. Enemy IO not only targets hardware and software, but also procedures, environmental controls, facilities, and personnel.

(a) Maintaining IA will be a continuing process throughout all phases of deployment and NETWORK operation. Commanders will employ all tools available to counter intentional and unintentional attempts to exploit friendly information and the command, control, communications and computer systems (C4S) systems transferring or processing friendly information.

(b) Commanders will take defensive actions necessary to protect the information processed and transferred over friendly C4 systems. Such protective measures may take the form of physical security, encryption, hardware configuration management, anti-jam and Electronic Counter-Countermeasures (ECCM) techniques, counter-deception, electronic and communications security, emission control procedures, OPSEC, deception, cover and camouflage, and use of low probability of detection and low probability of intercept communications.

(c) Particular attention will be given at all command levels to ensure the physical security and survivability of friendly command and control (C2) capabilities, the use of ECCM features to counter jamming, and the employment of deception, OPSEC, and other measures to counter intentional and unintentional attempts to exploit friendly C4 systems.

b. Tasks and Responsibilities

(1) Joint Force J1

(a) Follow basic AIS installation and operating requirements as described in this appendix.

(b) Follow AIS security measures as outlined in this appendix.

(c) Establish procedures for controlling foreign national network access in accordance with this appendix.

(2) Joint Force J2

(a) Follow basic AIS installation and operating requirements as described in this appendix.

(b) Follow AIS security measures as outlined in this appendix.

(c) Establish procedures for controlling foreign national network access in accordance with this appendix.

(3) Joint Force J3

(a) Follow basic AIS installation and operating requirements as described in this appendix.

(b) Follow AIS security measures as outlined in this appendix.

(c) Establish procedures for controlling foreign national network access in accordance with this appendix.

(4) Joint Force J4

(a) Follow basic AIS installation and operating requirements as described in this appendix.

(b) Follow AIS security measures as outlined in this appendix.

(5) Joint Force J6

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

(6) Supporting Combatant Commands (COCOM) and Major Commands (MAJCOM)

(a) Provide support as required.

(7) Defense Information Systems Agency

(a) Provide support as required.

(8) Commander, Marine Forces Component (MARFOR)

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

(9) Commander, Naval Forces Component (NAVFOR)

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

(10) Commander, Army Forces Component (ARFOR)

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

(11) Commander, Air Forces Component (AFFOR)

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

(12) Commander, Joint Special Operations Forces (JSOC)

(a) Establish Information Assurance (IA) and Information Security (INFOSEC) operations, in the context of Information Operations (IO), in accordance with this appendix and current cognizant references.

(b) Follow basic AIS installation and operating requirements as described in this appendix.

(c) Follow AIS security measures as outlined in this appendix.

(d) Establish automated software patch management systems and procedures as outlined in the appendix.

(e) Establish procedures for controlling foreign national network access in accordance with this appendix.

(f) Follow guidance provided in this appendix and applicable references for establishing AIS accreditation before connecting into live access networks.

(g) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(h) Report Information Assurance Vulnerability Alert compliance as required in this appendix.

c. Coordinating Instructions

Operational requirements to integrate physical security, communications security and AIS protection resources are clear. Commanders are responsible for ensuring strict adherence to cryptographic protection plans, ensuring physical protection activities are implemented at their respective locations and AIS are utilized in a multifaceted defense posture. Protecting critical command and control resources includes integration of all security programs and resources to counter enemy to our networks.

Tabs

A - INFORMATION SECURITY (INFOSEC)
B - NETWORK SECURITY
C - NETWORK MONITORING
D - ACCESS CONTROLS
E - ROUTER CONFIGURATION
F - FIREWALL POLICY
G - REMOTE ADMINISTRATION
H - INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA) POLICY
I - FOREIGN NATIONAL ACCESS TO NIPRNET AT COMPONENT SITES WITHIN THE JOINT AOR
J - CENTRIXS SECURITY
K - COALITION ACCESS TO CENTRIXS AT COMPONENT SITES WITHIN THE AOR
L - INCIDENT REPORTING (OMITTED)
M - WIRELESS ACCESS
N - CERTIFICATION AND ACCREDITATION
O - SYSTEM VULNERABILITY ASSESSMENTS
P - INFORMATION ASSURANCE ARCHITECTURE
Q – QUALITY OF SERVICE (QoS) POLICY

TAB A Information Security (INFOSEC)

1. Purpose

This tap provides direction and information to deny enemy efforts to exploit U.S. transmission systems and protect Essential Elements of Friendly Information (EEFI). This tab will describe information protection procedures aimed at both Communications Security and Information Security objectives.

2. General

The overall Joint Users Interoperability Communications Event 2006 Exercise Directive (JUICE 06) communications security (COMSEC) objective is to ensure transmission, cryptographic, emission, and physical security of information resources utilized by units operating communications equipment in this theater.

The NETWORKCOMSEC objectives will be obtained through specific actions designed to:

(1) Protect U.S. transmissions from hostile interception and exploitation.

(2) Secure transmissions by cryptographic systems that protect content from compromise through hostile crypto-analysis.

(3) Comply with appropriate application of physical safeguards that protect classified equipment, material, and documents from access or observation by unauthorized persons.

(4) Deny unauthorized personnel information, which may be derived from intercept and analysis of compromising emanations of crypto equipment or telecommunications systems.

The routing of unsecured U.S. communications throughout NETWORK via landline, high frequency radio, submarine cable, microwave, troposcatter, and satellites renders them vulnerable to intercept from numerous locations. Commanders at all unit levels will emphasize a total awareness of this vulnerability to their staffs.

COMSEC monitoring may be used during any access to the NETWORK. COMSEC monitoring results will be used to advise commanders immediately of security risks detected in transmissions, allowing them to counter possible enemy exploitation of compromised information.

The effectiveness of COMSEC is dependent upon the application of security in all phases of communications including communications planning, message drafting, transmission, and cryptographic and physical security policy compliance.

3. Execution

a. Concept of INFOSEC Support Operations

(1) Individual Service COMSEC policies apply.

(2) All personnel whose duties involve handling of classified information will be indoctrinated to ensure that they are fully aware of the consequences of inadequate COMSEC practices and of the types of information that must be protected during electrical transmission.

(3) Secure circuits will be used to the maximum extent possible.

(4) Only approved codes and authentication systems distributed through military department COMSEC channels are authorized for use within the Network.

(5) Use of non-secure telephones will be kept to a minimum. Secure telephone communications (such as, STE/STU-III, and DSVT) will be used whenever possible.

(6) Requests for COMSEC support to the foreign military (or any allied nation) must be done in accordance with Chairman, Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 54.

b. Tasks

(1) Joint Force J2

(a) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(b) Ensure INFOSEC considerations are an integral part of operational planning.

(2) Joint Force J3

(a) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(b) Ensure INFOSEC considerations are an integral part of operational planning.

(3) Joint Force J6

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Provide COMSEC call-out message, as required.

(f) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

(g) Assist component commanders with resolving combined INFOSEC issues.

(4) Supporting Combatant Commands (COCOM) and Major Commands (MAJCOM)

(a) Ensure INFOSEC considerations are an integral part of operational planning.

(b) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(c) Provide COMSEC call-out message, as required.

(d) Assist component commanders with resolving combined INFOSEC issues.

(5) Defense Information Systems Agency

(a) Ensure INFOSEC considerations are an integral part of operational planning.

(6) Commander, Marine Forces Component (MARFOR)

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

(7) Commander, Naval Forces Component (NAVFOR)

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

(8) Commander, Army Forces Component (ARFOR)

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

(9) Commander, Air Forces Component (AFFOR)

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

(10) Commander, Joint Special Operations Forces (JSOC)

(a) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP), as required.

(b) COMSEC violations will be reported via fastest secure means available, in accordance with component service regulations.

(c) Ensure INFOSEC considerations are an integral part of operational planning.

(d) Establish cryptographic distribution authorities and request use of the Joint Inter-theater Communications Security (COMSEC) Package (ICP) as required.

(e) Develop, in accordance with provisions of the cognizant COCOM, Department of Defense (DOD) and Service directives, an acceptable level of communications security with allied forces engaged in coalition operations.

c. Coordinating Instructions

(1) NETWORK user commands are responsible for engineering, installing and operating their portion of the NETWORK in accordance with policy and procedures established in the basic appendix.

(2) COMSEC material required to access the NETWORK will normally be satisfied from established service resources.

4. Administration and Logistics

Not Applicable.

5. Command and Control

Security violations will be analyzed and dealt with expeditiously in accordance with NSTISSI-4003 and appropriate supplements as indicated:

a. US Army - AR 380-41

b. US Navy/USMC - CMS-1A

c. US Air Force - AFKAG-1M

Exhibits: NA

TAB B Network Security

1. Purpose

The purpose of this tab is to prescribe policies, procedures and responsibilities for use of the Secure Internet Protocol Router Network (SIPRNET), Combined Enterprise Regional Information Exchange System (CENTRIXS), Non-secure Internet Protocol Router Network (NIPRNET), Internet, and electronic mail (e-mail) in the NETWORK environment.

2. Policy

The Internet and/or World Wide Web (WWW) enables users to obtain and exchange unclassified information globally. References to the Internet and WWW will be collectively termed "Internet" in this document. Access to the Internet can benefit the spectrum of US military operational, administrative, and morale, welfare recreational mission requirements. Access to information services on any Internet is granted for authorized use only. Such use will be monitored to ensure protection of networks and information and to verify compliance with these instructions. All DOD network users are subject to unannounced network inspections or network monitoring. Similarly, SIPRNET and CENTRIXS provide search and retrieval of classified or otherwise sensitive information available on those networks, and all policy herein shall be considered applicable to users and administrators of CENTRIXS and SIPRNET.

3. Usage

a. All DOD AIS users, particularly supervisory personnel, must continually promote the safe, effective, efficient, and legal use of US Government resources.

(1) Personnel must exercise the highest standards of professionalism and responsible behavior with the information they obtain from or make available on the Internet.

(2) Personnel must exercise caution and protect information that foreign governments, or others might use to the disadvantage of the US Government. This information may include operationally sensitive, and/or classified information.

(3) Personnel must assume that "public" Internet computers can be accessed by anyone worldwide and take action to protect information against unauthorized disclosure.

(4) Personnel must take measures to eliminate the risk of unauthorized disclosure of classified data while utilizing DOD AISs.

b. NETWORK AIS users fall under DOD 5500.7-R, Joint Ethics Regulation (JER), Section 2-301 (Change 2) dated 22 March 1996. The JER requires that the use of government communications systems and equipment (including computers, electronic mail, and Internet

systems) "shall be for official use and authorized purposes only." Commanders must ensure that all users are fully aware that there is **no expectation of privacy on/within DOD networks.** This policy shall be reflected in unit level policy and user access agreements.

(1) Official Use. Official use refers to use that directly furthers the interests of DOD and the duties prescribed for the individual position.

(2) Authorized Purposes. Authorized purposes refer to personal use within specified limits as permitted by an appropriate level supervisor so as not to impact the organization or individual's job function or mission.

c. Before authorizing personal use of DOD AISs, a supervisor must determine/verify that the use:

(1) Does not adversely affect the performance of official duties by the DOD employee or the DOD employee's organization.

(2) Is of reasonable duration and frequency and occurs during an employee's personal time (before/after duty hours, during lunch or authorized breaks).

(3) Serves a legitimate government interest.

(4) Is not used for purposes that adversely reflect upon DOD, or the Federal Government.

(5) Does not overburden DOD computing resources or communications systems nor result in added costs to the Government.

d. Authorized purposes for limited personal use include the following e-mail or web-based activities:

(1) E-mailing short personal messages to a relative or colleague.

(2) Receiving e-mail (as long as comparable receipt would be acceptable via telephone and is no more disruptive than a telephone call).

(3) Making a medical, dental, auto repair, or similar appointment.

(4) Improve professional or personal skills as part of a formal academic, education, military or civilian professional development program (when approved by an immediate supervisor). In accordance with the provisions of Tab F of this appendix, requests to modify firewall/router Access Control List (ACL) configurations for the sole purposes of access to educational sites or services, must be requested via the Local DAA to forward for approval.

(5) Serves a legitimate public interest such as enhancing professional skills, educating personnel in using the system, improving morale of personnel stationed

away from home for extended periods, or job-searching in response to military retirement or Federal Government downsizing.

4. Prohibited Use of Network Services

a. Violating the prohibited uses/appropriate use agreement of the NIPRNET/Internet, CENTRIXS, or SIPRNET can result in administrative action, or judicial or non-judicial punishment in accordance with federal law, the Uniform Code of Military Justice, and civilian employee regulations. The use of Data Network services in the following types of activities is specifically prohibited by any and all NETWORK extended network users:

(1) Activities with purposes for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, advertising, or sales of personal property.

(2) Fundraising activities for commercial, personal, or charitable purposes. (Official morale, welfare, recreation, officer and enlisted aid activities are authorized.)

(3) Using NETWORKAIS networks as a staging ground or platform to gain unauthorized access to other systems (hacking).

(4) Opening e-mail attachments from unknown or questionable sources or opening attachments from other sources without downloading to disk and virus scanning.

(5) Creating, copying, forwarding or transmitting chain letters or other unauthorized mailings or solicitations, regardless of the subject matter. This prohibition includes virus warnings – receipt of such warnings should be forwarded to the Component IA Officer or Manager only.

(6) Accessing, creating, downloading, viewing, storing, copying, processing, displaying, or transmitting sexually oriented, hate, or racist materials.

(7) Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist/terrorism activities, Extremists/ Extremism activities, any illegal activities, or other activities otherwise prohibited.

(8) Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

(9) Posting DOD information to external newsgroups, bulletin boards, or other public forums without authority.

(10) Accessing sites with continuous unofficial data streams (such as, audio or video such as Pointcast) shall not be permitted. Webcam use requires local DAA written permission on a case-by-case basis due to the bandwidth utilization that this

capability may cause. Use of Web-cams to communicate externally from the deployed enclave requires approval of theater Combatant Command (COCOM) J6.

(11) Accessing sites known for hacker attacks or hacker activity or that are hostile to the US. This does not apply to Intelligence and Information Assurance personnel when accessing these sites for official use. To limit exposure of the network to hostile actions and monitoring, access to these sites will be made from special systems placed in a DMZ or when available, a separate commercial connection.

(12) Accessing or participating in commercial messaging, instant messaging, or unauthorized Internet Relay Chat or other "Chat" sessions. Exceptions are granted for DOD and Service authorized collaborative planning tools or Service-provided Government-off-the-shelf capability used for official business. MWR usage is not an authorized exception unless the connection is provided by a separate commercial link not connected to the NIPRNET.

(13) Downloading and/or installing shareware/freeware software or other non-approved executable programs (for example, .EXE, .COM, .BAT, or script files) for non-DOD approved functions. This includes, but is not limited to, gaming software, file sharing software such as KaZaA, Morpheus, Napster, BearShare, Gnutella, AudioGalaxy, Limeware, or Winmx, and instant messaging software such as AOL Messenger and Yahoo Messenger or any of their Components. Non-approved applications such as these use tremendous amounts of network bandwidth and have the potential of providing a gateway for malicious activity that could compromise our networks. Only DOD, Service, or COCOM approved Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) software, or DOD or COCOM-approved or freeware/shareware (such as, Adobe Acrobat Reader), shall be permitted. The authorized or unauthorized use of file-sharing applications does not relieve in any way the Service, Unit Commander or individual user from US and International copyright protection laws. Unit Commander's shall take careful regard to personal legal liabilities prior to accepting these applications into their networks as "morale and welfare" initiatives.

(14) Participating in "spamming," that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

(15) Participating in "letter bombing"; that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail.

(16) Storing, processing, or distributing classified, proprietary, or other sensitive or For Official Use Only (FOUO) information on a computer or network not explicitly approved for such processing, storage, or distribution.

(17) Using another person's account or identity without previously obtained explicit permission (such as, forging e-mail).

(18) Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.

(19) Attempting to circumvent or defeat security or auditing systems without prior authorization. This use is only authorized as part of legitimate system testing or security research.

(20) Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyrights, trade secret, or license agreement.

(21) Allowing any unauthorized person to access a DOD-owned system through the authorized users account or by creating a new account for the unauthorized user. Authorization for SIPRNET, CENTRIXS, or NIPRNET access can be granted only by the appropriate organization designated to maintain network accounts as determined by the local DAA. Use of Government stand-alone systems that do not at any time connect to the SIPRNET, CENTRIXS, or NIPRNET are under the control cognizance of the local Commander or their appropriately designated personnel.

(22) Modifying or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

b. The policy outlined in DOD 5500 specifically addresses appropriate uses of AISs and clearly states to all users that there is no reasonable expectation of privacy while using DOD AISs. Appropriate security offices are responsible for and routinely conduct monitoring of E-mail as well as content searches of data files stored on individual or network storage devices. This includes searching and potentially seizing data files. The user assents to such monitoring by accessing the AIS, in accordance with the DOD warning banner. It is imperative that users who desire information to remain private use external, personally owned computers and Internet service providers outside the government working facility.

5. Responsibilities

a. Supervisors must monitor subordinates using DOD Data Networks, Internet Access, and computer resources to ensure that the guidance in paragraphs 3.c. and 3.d. are followed. Network uses noted above are a privilege, not a right. Supervisors may revoke the authorized personal use of Internet or other network services noted above, or parts thereof, for any perceived misuse of DOD resources.

b. Employees, including Military, Government, Contractors and non-US authorized users, shall use DOD communications systems with the understanding that:

(1) Use of such systems serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

(2) Use of such systems is not anonymous. For each use of the Internet or any DOD Network, the name and computer address of the employee user can be recorded, as well as the Internet locations visited.

(3) Most Government communications systems are not secure. Employees shall not transmit classified or otherwise sensitive information over any communication system unless approved security procedures and practices are used (such as, appropriate encryption, secure networks/workstations).

(4) Users shall not disclose communications system access or authentication data (such as passwords) to anyone, unless such disclosure is authorized by appropriate authority.

(5) Users shall use extreme care when transmitting sensitive information or other valued data. Information transmitted over an open network, such as e-mail, the Internet, telephone or fax, is accessible to anyone else on the network. Information transmitted through the Internet or by e-mail is accessible to anyone in the chain of delivery, and may be re-sent to others by anyone in the chain.

(6) All electronically transmitted information, including e-mail, can become part of official government records, which may be released under the Freedom of Information Act.

(7) In order to ensure that authorized personal use does not adversely affect the performance of official duties, personnel may only go online when needed and must immediately disconnect (close their browser) when they are finished. Users must terminate and log off on completion of their business in order to share hardware resources in multi-user environments. Do not leave Internet connections running throughout the day. Remote dial-in access may only be used for official use (such as, mission-related dial-in from home or TDY location). Personal use of the dial-in capability is prohibited.

(8) Users shall not connect non-DOD equipment to government networks except as permitted in paragraph 3.g (6).

6. Electronic Mail (E-Mail)

All use of e-mail must comply with DOD policies and directives.

a. All personnel must ensure that the content of their e-mail messages is professional and does not misrepresent or misstate DOD positions or policies either through content, context (inference) or association.

b. Release of e-mail addresses is in compliance with DOD Regulation 5400.7-R. For the purposes of the Freedom of Information Act, COCOMs are placed under the jurisdiction of the Office of the Secretary of Defense, not the administering Military Department (paragraph

AP1.1, DOD Regulation 5400.7-R). Withholding the release of e-mail addresses may apply to military and/or civilian personnel assigned to units that are sensitive, routinely deployed, or stationed in foreign territories.

c. Cognizant COCOMs routinely monitor e-mail **content** to support Operational Security (OPSEC) programs. For this reason, no communication via a NETWORKAIS shall be considered "private."

d. Under no circumstances shall unit commanders endorse, condone or approve the use of commercial e-mail services to support DOD business. Automatic forwarding of e-mail to commercial e-mail services for the purposes of conducting or supporting official DOD business is also explicitly prohibited.

7. File Transfers

Users will not download software of any kind. All authorized software that is introduced onto NETWORK connected systems must be procured, evaluated and installed by applicable authorities.

a. Shareware, like commercial software, may be purchased and used when properly obtained through established Component acquisition processes, tested for network compatibility and vulnerabilities, and installed by System Administrator personnel.

b. Obtaining executable software from FTP sites outside DOD and other governmental agencies is prohibited unless part of the acquisition process per paragraph 7.a.

c. Transfer of files over the NIPRNET will utilize PKI encryption where possible.

8. Internet Chat

Commercial/personal uses of internet chat are not approved on NETWORK connected networks. Paragraphs 4.a.(12) and 4.a. (13) of this Tab addresses this subject.

9. World Wide Web (WWW)

Component personnel have access to the WWW and Internet via the NIPRNET. The WWW is the primary means that deployed commands can use to share releasable information with the general public. As such, all deployed organizations and activities maintaining a public web presence through the NETWORK will comply with the following procedures:

a. The Home Page on any Component network web server is official and must conform to established page design and performance standards. Components will appoint a web site point of contact that will ensure that the information provided is professional, accurate, and current.

b. All information presented on the WWW is the direct responsibility of the Commander who sponsors the web page. These persons must ensure that all information is kept current and accurate.

TAB C Network Monitoring

1. Purpose

The purpose of this tab is to establish policy for monitoring of NETWORK accessed AIS systems and networks. The focus is on monitoring, auditing, and management of AIS networks to enhance awareness of the operating situations, status and indications of security problems, and responsibilities.

2. Background

a. There is an established requirement for continuous monitoring and reporting of the Information Assurance (IA) posture of DOD networks.

b. Certain laws authorize the Government, including DOD, to monitor telecommunications (in transit) and stored data on electronic systems:

(1) Government intercept of telecommunications is lawful where the government official is a party or there is consent.

(2) Service providers, (including DOD), are exempt from provisions against unauthorized communication intercept in certain instances. Title 18USC2511 states "It shall not be unlawful under 18USC2511 for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service. Or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

(3) Government telecommunications systems shall be subject to Communications Security (COMSEC) monitoring by duly authorized government entities. Theater Combatant Commanders (COCOM) authorize and use resources from the National Security Agency (NSA) and other Government organizations to perform specific monitoring tasks (as specified by individual department or agency regulations). Users of these systems must be properly notified in advance that system usage constitutes implied consent to active monitoring of NIPRNET and telephone transmissions for OPSEC or COMSEC purposes. 18 USC Sec 2511(2)(d) states that monitoring only requires consent of one of the parties of the communication.

(4) The Electronic Communications Privacy Act (ECPA) gives a service provider, (including DOD), the right to access stored information. Deployed AISs accessing network services through the NETWORK are not accessible to the general public. As a private network infrastructure, the resources are provided for the sole purpose of

accomplishing US COCOM operational missions. Personal use, in limited form, may be authorized as stated in Tab B, paragraph 3 of this appendix.

(a) There are established requirements to conduct periodic reviews of the adequacy of the safeguards for operational, accredited AISs. To accomplish this there must be an audit trail. Audit trails will be reviewed daily when possible, or as a minimum weekly by IA security analysts or System Administrators.

(b) Commanders shall establish procedures to assure that each deployed AIS accessing the NETWORK is subject to a minimal audit as described below:

1) Periodic reviews of the adequacy of the safeguards for operational accredited AIS shall be conducted.

2) There will be a detailed audit trail providing a documented history of AIS use to ensure that events may be reconstructed to ensure each person having access to an AIS may be held accountable for his or her actions on the audit.

3) The manual and/or automated audit trail shall minimally document the following:

a. Identity of each person and device having access to the AIS.

b. Time of the access.

c. User activities sufficient to ensure user actions are controlled and open to scrutiny.

d. Activities that might modify, bypass, or negate safeguards controlled by the AIS.

e. Security-relevant actions associated with periods where the processing or changing of security levels or categories of information has occurred.

(c) TASOs shall implement audit capabilities on all system network servers and identify applicable audit procedures.

1) Network events will be audited using operating system audit or 3rd party automated features to identify at a minimum:

a. Date and time of the event.

b. User.

c. Type of event.

d. Success or failure of the event.

e. The origin of the request.

f. The name of the object introduced, accessed, or deleted.

g. The sensitivity determination of the object.

2) Audit mechanisms systems must comply with DISA Security Technical Implementation Guide (STIG) minimum requirements, including but not limited to the following:

a. Allow the review of patterns of access to individual objects, access histories of specific processes and individuals, and the use of the various protection mechanisms supported by the system and their effectiveness.

b. Allow discovery of both user and outsiders' repeated attempts to bypass the protection mechanisms.

c. Allow the discovery of any use of privileges that may occur when a user assumes functionality with privileges greater than his or her own, such as, programmer to administrator. In this case there may be no bypass of security controls but nevertheless a violation is made possible.

3) The system shall be analyzed for proper, correct, full and complete implementation of auditing.

(d) Each network will be monitored continually by automated mechanisms to obtain, display, and record the current and historical operating and security status of the network.

1) Monitoring mechanisms will provide information not only on conventional system/network status, but also will make available data concerning those events that have security importance.

2) More than one particular type of monitoring tool or device will be used. More than one automated audit or monitoring mechanism (software application, tool) should be used.

3) Network packets (traffic) will be actively monitored for content and key signature. This monitoring requirement is to provide specific

conduct and support the enforcement of appropriate use policy. Active monitoring is hereby defined as "real-time" and/or "near-real time" review of network activity.

3. Policy

a. A warning banner will be displayed at logon to all NETWORK (or DOD) connected networks advising that all users may be subject to monitoring. Warning Banners shall require the user to accept the Warning Banner conditions before continuing with the logon. A Warning Banner example is provided in Tab J paragraph 4 for CENTRIXS and paragraph 3.e.(9) of the main body of this appendix for all other networks.

b. Periodic reviews of all AIS safeguards will be conducted.

c. Where Dynamic Host Configuration Protocol (DHCP) or Network Address Translation (NAT) are used, auditing must be capable of identifying a specific user and equipment location for the last 24 hours. To assist this requirement, lease rates for DHCP are recommended to be set no shorter then 8 hours. NAT should be avoided if at all possible and any system using NAT must clearly state this on their network diagrams during the accreditation process.

d. Any known or suspected compromise of AIS security will be reported immediately to the responsible TASO who will forward the report, without delay, through the chain-of-command to the cognizant COCOM Information Assurance Manager IAM. The COCOM IAM will prescribe the immediate corrective action and file appropriate reports of Service Chains and J6. Further incident reporting policy may be found in Tab L of this appendix.

e. Intrusion Detection Systems (IDS) will employ active defensive capabilities to retain network protective postures and prevent rapid spread of intrusions and virus attacks. Careful coordination with deployed Commanders is required to ensure the highest level of protection while maintaining operational capability of critical C2 systems.

4. Responsibilities

a. Terminal Area Security Officer (TASO) Responsibilities

(1) The TASO conducts security audits for operational systems as well as for systems under development. The TASO also monitors variances in security procedures and reviews any relevant audit trail data from the system. The TASO provides senior management with reports on the effectiveness of security policy, identifies weaknesses, and makes recommendations for improvements.

(2) The audit trail provides a record of system security-related activity and allows the TASO to monitor activities on the system. If manual audits are necessary, the TASO shall document random checks made to verify that users are recording system usage. Audit trail files must be protected to prevent unauthorized changes or destruction.

(3) Besides the system audit trail, network audit reports can provide detailed information on network traffic and provide summary accounting information on each user ID, account, or process. Specifically, the TASO will:

(a) Select security events to be audited. Ensure that the audit trail is reviewed and have the capability to audit every access to controlled system resources (such as, very sensitive files). Archive audit data.

(b) Develop and implement audit and review procedures to ensure that all AIS functions are implemented in accordance with applicable policies and programs. Existing policies and programs usually establish the minimum amount of material that shall be audited.

(c) Conduct audits and maintains documentation on the results.

(d) Supervise review of security audit parameters. Develop, review, revise, submit for approval, and implement procedures for monitoring and reacting to security warning messages and reports.

(e) Conduct random checks to verify compliance with the security procedures and requirements.

(f) Gather information from audit trails to create profiles of system users. Observe user patterns such as the terminal usually used, files accessed, normal hours of access, and permissions usually requested, to determine which actions are unusual and shall be investigated.

(g) Review audit trail reports for anomalies:

1. Multiple unsuccessful logon attempts. This could be an indication of an inexperienced user, a user who has recently changed passwords and forgotten the new one, or an attempted intrusion.

2. Attempt by a user, who is already logged in at a terminal, to log in again to the same system from a second terminal. This could be caused by an inadvertent failure to log out at the first terminal, an intentional logon to both terminals, and an attempted intrusion.

3. Individuals logging in after normal hours. This may mean the user has a deadline to meet and is working overtime or that an intruder is attempting access.

4. High numbers of unsuccessful file accesses. This could be prompted by user failure to remember file names or by an attempted intrusion.

5. Unexplained changes in system activity.

6. Covert channel activity

(h) Audit trails must be reviewed weekly at a minimum, but preferably daily. Depending on the size of the system, the review can consist of the entire audit trail or of a review of customized reports.

(i) Audit trail files must, whenever possible, be protected by encryption. Access must be controlled to prevent unauthorized access, tampering, or loss.

(j) Audit trails must be maintained for one year in either paper or electronic form.

(k) Paper copies of audit trails should be treated as *FOR OFFICIAL USE ONLY* and shredded when no longer needed. Electronic copies must be cleared in some manner before disposal.

(l) The TASO should monitor all Transmission Control Protocol/Internet Protocol (TCP/IP) activity with a Network Intrusion Detector/Joint Intrusion Detector (NID/JID) system, or other Service-procured Commercial-off-the-shelf Intrusion Detection System (IDS). The STEP IA Tool suite will be utilized on all STEP/Teleport connections when it becomes available. Service components are encouraged to install their own service provided IDS system as an additional layer of protection especially on passive JIDS/SNORT (*Snort® is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods.*) protected STEP/Teleport connections.

b. Network Management/Monitoring Station

(1) The management workstation must be located in a secure environment with only limited access.

(2) Only those accounts necessary for the operation of the system and for access logging should be maintained.

(3) A record of all logins and transactions processed by the management station must be kept. Include time logged in and out, devices that were accessed and modified, and other activities performed.

(4) Access to Network Management Stations will be restricted to known authorized users with appropriate user ID and password. Encryption should be used for passwords and entire network management sessions (such as – system encryption or SSH client). *(SSH client is a program for logging into a remote machine and for*

executing commands on a remote machine. It is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network.)

This page intentionally left blank.

TAB D Access Controls

1. General

a. Policy for System Access Control

(1) There shall be an access control policy for each Automated Information System (AIS).

(2) The features and/or procedures of the access control policy are to be applied so as to enforce the security policy set to protect the information within the AIS. Files that have restricted need-to-know information will have additional safeguards to prevent general access (such as restricted and protected subdirectories and files).

(3) The identity of each authorized user shall be established positively before system access is granted.

b. Background

(1) Access and Access Control

(a) Access is the opportunity to make use of an information system resource.

(b) Access control is limiting access to information system resources only to authorized users, programs, processes, or other systems.

(c) An access control mechanism is a security safeguard designed to detect and deny unauthorized access and permit authorized access.

(d) An access control list (ACL) is a mechanism implementing discretionary and/or mandatory access control between subjects and objects.

(2) Identification

(a) Identification is the process employed within the AIS to recognize an entity.

(b) A user identification (USERID) is "A unique symbol or character string that is used by an AIS to identify a user."

(3) Authentication

(a) Authentication is a security measure to verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise

exposed to unauthorized modification in an information system, or to establish the validity of a transmission.

(b) An authenticator is a means used to confirm the identity of a station, originator, or individual.

(c) Authentication can be based on any one or combination of three factors of information: something the person knows (such as, a password); something the person possesses (such as, a card or key); something unique about the person (such as, fingerprint, retina, or voiceprint). Three-factor authentication would require all 3 factors of information to validate the user.

(d) An identity token is something a person possesses (such as, Common Access Card (CAC), smart card, metal key, or other physical object used to authenticate identity).

(e) Identity validation enables an information system to authenticate users or resources.

(4) Password. A Password is a protected string of characters that identifies or authenticates a user. Knowledge of the password is considered proof of authorization to access a system. Passwords will be unique for each network system accessed to prevent compromise of one password allowing access to multiple network systems. A password is composed of a minimum of eight characters combining the characteristics of upper case and lower case letters, numbers and special characters.

EXAMPLE: 1abCD$234

2. Identification

a. Network systems must identify individual users by means of a USERID and authorize access through the use of a unique password. The USERID is unique and should clearly identify the individual. If the USERID refers to a duty position it still must be used by a single identifiable person and the password changed when the person holding the duty position changes.

b. USERIDs will not be used for more then one individual. Exceptions to this can be made in writing by the DAA for a very limited number of terminals where a group of individuals share a terminal for a common duty purpose like a watch position. This exception must list the individual users and the mission imperative that requires this exception. If an exception is approved a written record must be available to show when each individual was accessing that system. Exceptions will not be granted for convenience or for shared terminals where individual USERIDs are possible. This exception should not exceed 1% of all users and does not apply to CENTRIXS.

3. Authentication

All network systems must authenticate through a combination of the user's USERID and password. The USERID allows the network manager to audit individual user usage. Only the user knows his/her unique password. The password allows access to the network resources authorized to the user.

4. Access Control Principles

a. The AIS shall be configured with the principle of least privilege, so that each user only has access to all of the information to which the user is entitled (by virtue of clearance and formal access approval). In the case of "need-to-know" for classified information, access must be essential for accomplishment of lawful and authorized government purposes.

b. Approval by a data owner to allow access by another user to a particular item or category of information will be formally documented as a Formal Access Approval.

5. User Responsibilities

a. Prior to receiving AIS access, all personnel will receive AIS security indoctrination upon initial assignment.

b. Users will not write down passwords (such as, to store in a wallet or desk-drawer).

c. Each user will inform the TASO when accesses to particular AIS or networks are no longer required.

d. The user will not divulge either USERID or passwords to any other unauthorized person or organization unless the network manager under extenuating circumstances authorizes such disclosure.

e. Each user will immediately report any possible compromise of a password to the TASO.

6. Password Generation

Upon account approval, the initial password is randomly generated and provided to the user. Initial user logon must require the user to generate their own unique password.

7. Password Characteristics

a. Passwords will be comprised of a minimum of 8 characters.

b. Passwords must contain each of the following character qualities:

- Alphabetical UPPERCASE letters.
- Alphabetical lowercase letters.
- Numbers (0,1,2,3,4,5,6,7,8,9)
- Special characters (#, &, <, /, %, ?, etc.).

c. Passwords will not consist of any proper names, words from fictional stories or movies, or words that can be found in standard dictionaries (such as the *Oxford English Dictionary*, or the Merriam-Webster's *International Dictionary*).

d. Repeated, consecutive characters will not be permitted.

e. User-generated passwords must be examined at time of creation, via software or inherent OS capability, for compliance with paragraph 8.b. Passwords must be checked periodically to identify weak password and passwords that do not conform to the requirements in paragraph 8.b. (such as, an automated "password cracker" program).

8. Password Lifetime/Duration

a. Under normal circumstances, users will not be permitted to change passwords more than once in a 24-hour period.

b. Passwords age will never exceed 90-days from the time of creation. Users will be automatically notified of pending password expiration 14-days in advance of expiration. The notifications will continue until the user changes their password or the account is disabled because the password has expired. Any password used within the last 24 password changes will not be accepted as a valid password and the system will prompt the user for a new, unique password.

c. User accounts will be deleted when a user is no longer with the sponsoring organization.

d. Inactive user accounts will be identified and deleted. Unit policy shall define reasonable criteria for determining if an account is no longer required.

e. All USERIDs will be revalidated periodically, at least once every 90 days.

9. Automatic Disabling of Accounts

a. The user account will be disabled after three consecutive unsuccessful log on attempts. The user must contact the administrator to validate their password or change an expired password. Login attempts are not cumulative and will reset at a successful login.

b. Logon attempt rates will be limited. The maximum login attempt rates will be established within the range of one per second to one per minute. This is to control the number of attempts a potential attacker can make during a password lifetime through a single access port.

10. Security of Passwords

a. Only the individual user is authorized to know the password of his/her account. The one exception to this is for watch-standing accounts. Watch accounts require active account users to share time-slices of accountability, depending on the log entries and the watch shift.

b. The user must sign a receipt (user agreement) for the initial password. The receipt must contain an acknowledgment that the user understands the responsibility to protect the password and has received guidance on password selection. Password receipts shall be kept on file for as long as a user has access.

c. System and network management files containing lists of system account passwords will be encrypted and provided the same level of protection as the functions/data on the system on which the password is used. Access to system and network management files containing lists of passwords will be limited to those persons who are authorized access.

d. Passwords that must be documented will be secured commensurate with the level of access they provide.

e. Passwords will be applied to all configuration levels within communications servers and access ports, regardless of functionality or lack thereof (such as, console, auxiliary, TTY, etc.).

11. New System Defaults and Backdoors

a. Vendors often program code-activated bypasses (known as "backdoors") for their own use to troubleshoot the systems they support. All vendor backdoors and any known vendor USERIDs and passwords will be removed from the system prior to installation on NETWORKaccess networks.

b. Non-essential system default accounts will be deleted or disabled.

c. Prior to installation on the network, default passwords will be changed.

12. Compromise and Password Replacement

a. When a system has been compromised and the possibility exists that user passwords may have been disclosed, system users will immediately change their password.

b. Suspected or verified password compromises will be reported immediately through the Terminal Area Security Officer (TASO).

c. Passwords shall be deleted or replaced immediately when that owner is no longer an authorized AIS user or any one of a set of owners is no longer authorized access to the data

d. Passwords forgotten by their owner shall be replaced, not reissued.

13. Passwords on Communication Servers

a. Communications servers allow asynchronous devices, such as terminals, printers and PCs, access to a LAN infrastructure. Communications servers usually have one connection to the

LAN and multiple incoming ports connected to modems. These modems can handle dial-up calls or dedicated lines from remote sites. Remote dial-in access to NETWORKaccess networks is discouraged, and requires stringent authentication, encrypted communications through public networks, regardless of the Network accessed, and a network intrusion detection sensor on the inside of the communication server.

b. All levels of the configuration within the communications server will be password protected.

c. All access points (ports) will have passwords, regardless of functionality or lack thereof (such as, console, auxiliary, or teletype [TTY]).

d. Different passwords will be assigned to the view option and the write option portions of the communications server.

14. Passwords on Routers

a. All access points (ports) will have robust passwords, regardless of functionality or lack thereof (such as, console, auxiliary, TTY, or line).

b. All router levels (privileged and non-privileged) will be password protected.

15. Passwords and Dynamic IP Address Assignment

Supplemental Identification and Authentication (such as USERID and password) will be implemented if dynamic Internet protocol address assignment is employed.

16. Workstation/Monitor Screen-Blacker/Screensaver Passwords

Users will invoke the password protected screensaver when away from their workstation. Systems will be configured to activate the screensaver after no more than 15 minutes of inactivity.

TAB E Router Configuration

1. Purpose

The purpose of this tab is to establish policy for employment of routers within networks and systems accessing and the network. Waivers to this policy must be submitted through the cognizant theater COCOM J6.

2. General

This tab establishes the policy for security configuration of routers and similar capabilities regarding configuration control and management. It also defines what types of incoming telecommunications are permitted and/or not permitted to enter the controlled perimeter. Only TCP/IP (Transport Communications Protocol/Internet Protocol) networks (Internet, NIPRNET [Non-classified Internet Protocol Routing Network], the Secret Internet Protocol Routing Network [SIPRNET]), and CENTRIXS are considered. Further guidelines may be found in cognizant theater COCOM Network Operations and/or Ports and Protocols guides. Security Architecture and placement may be found in Tab P to this appendix.

3. Background

(1) The U.S. National Communications System, Federal Standard *1037C Telecommunications: Glossary of Telecommunication Terms* (07 August 1996) describes the term router as follows: "In data communications, a functional unit used to interconnect two or more networks. Routers operate at the network layer (layer 3) of the International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model. The router reads the network layer address of all packets transmitted by a network, and forwards only those addressed to another network."

(2) Within the network AIS, the router functions as an inter-network device, which determines the route, a packet must take and forwards the packet to its destination. Routers function on the principle of Route Cost, and use the information stored in the Routing Table to determine the best path for a packet. This process applies to any routing protocol implemented including link-state and distance vector protocols.

4. Filtering by Source or Destination Address

a. Background. The perimeter/border router is the point of entry to a site for all packets or IP data-grams from the DISN. Thus, it is the first place where packet filtering or monitoring can be performed under the control of the site. This device has the capability of performing packet filtering using basic filtering rules.

b. Routers will be configured to reject inbound packets from addresses that are known or likely originators of computer network attacks.

c. Routers will be configured to reject outbound packets that are addressed to suspect addresses.

d. Traffic will be restricted to known routers within the cognizant theater COCOM's architecture and to known and trusted external systems.

e. The router will be configured, if possible, to audit and alarm for unknown routers attempting to protocol handshake.

5. Filtering by Traffic Destination Port or Requested Service

a. Background

(1) Streams of incoming TCP/IP packets contain information about the destination port - a value at the transport layer that serves as a software-based "point of access" to the system to distinguish among the multiple applications that may have connections with a single host. Various communications protocols that implement requests for functions (services) are by convention associated with a destination port number. Thus, blocking a port equates to blocking the protocol and the request for the service. This type of access control is needed to prevent both external and internal security breaches (such as, one department should not be able to access another's database).

(2) Routers shall be configured to "deny by default." such as deny all ports/protocols that are not explicitly allowed.

b. The following will be blocked at all network border routers:

(1) All spoofing holes, local host, 255.255.255.255, 0.0.0.0 (Ref: ASSIST Bulletins 95-01, 95-29, 95-51, and CERT Bulletin 96-21)

(2) All Internet Control Message Protocol (ICMP) except *Ping* and *Traceroute* (Ref: ASSIST Bulletins 95-01, 95-29, and 95-51.)

(3) All source routed packets

c. The following Ports and Services Filtering Table is the network standard for router configuration.

PORTS AND SERVICES FILTERING TABLE (Version 9.03)

Key to Table Entries	
Allow	Without this service the system will not be fully functional.
Block	Possible source of entry for attack. Disallow unless absolutely necessary and alternate protection is available
=	Service is harmless. Block or allow.
*	Allow where service is needed. Block if not needed.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
1	TCP	TCPmux	Block	TCP Port Multiplexer. Rarely used; deny service by blocking this port.
7	TCP	Echo	*	An echo server that can be useful for seeing if a machine is alive. A higher-level equivalent of ICMP echo (ping).
7	UDP	Echo	Block	
9	TCP;UDP	Discard	=	The /dev/null of the Internet. Harmless.
11	TCP	Systat	Block	Occasionally connected to netstat, w, or ps. a.k.a. USERs protocol; returns active users.
13	TCP	Daytime	=	Daytime.
13	UDP	Daytime	Block	
15	TCP	Netstat	Block	See systat.
18	TCP	Msp, v2	Block	Message Send Protocol. See RFC 1312 for security considerations.
19	TCP;UDP	Chargen	=	Character Generator.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
20	TCP	ftp-data	*	Data channel for ftp. Hard to filter. Relevant CERT Advisories: 97-27, 97-16, 94-08, 94-07, 93-10, 93-06.
21	TCP	ftp	*	FTP control channel. Allow only to your FTP server. See the CERT advisories listed under ftp-data.
23	TCP	Telnet	*	Telnet. Relevant CERT Advisories: 95-14, 95-03.
25	TCP	Smtp	*	Simple Mail Transfer. See CERT advisory 95-05 for send mail vulnerabilities.
37	TCP;UDP	Time	=	Time of day in machine-readable format.
43	TCP	Who is	*	Who Is. Allow in only if who is server is sanitized.
49	TCP	Login	*	Login Host Protocol. See CERT Advisories 97-15, 97-06, 94-09, 93-12, 91-08 and ASSIST bulletins 94-19, 93-24.
53	TCP;UDP	Domain	Allow	Domain Name Server. Restrict TCP access to port 53 to known secondary domain name servers to the extent possible.
65	TCP	Tacacs-ds	=	TACACS-Database Service.
67	UDP	Bootp	Block	Bootstrap Protocol Server.
68	UDP	Bootpc	Block	Bootstrap Protocol Client.
69	UDP	tftp	Block	Trivial File Transfer. See CERT advisories 91-18, 91-19.
70	TCP	Gopher	*	Gopher server. Can be dangerous. Use with caution. See CERT advisory 93-11 and ASSIST bulletin 93-21.
71	TCP	Netrjs-1	Block	Remote Job Service.
72	TCP	Netrjs-2	Block	Remote Job Service.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
73	TCP	Netrjs-3	Block	Remote Job Service.
74	TCP	Netrjs-4	Block	Remote Job Service.
77	TCP	rje	Block	Any private RJE service.
79	TCP	Finger	Block	Finger. See CERT advisory 93-04 and ASSIST bulletin 93-06.
80	TCP;UDP	Www-http	*	See CERT advisories 97-07, 95-04 and ASSIST bulletin 95-06.
87	TCP	Link	Block	Commonly used by hackers. A nice place for an alarm.
88	UDP	Kerberos	*	If logins are allowed, whether directly or via inter realm authentication, this port must be open. Otherwise it should be blocked.
95	TCP	Supdup	*	SUPDUP. Hackers port. Good place for an alarm.
102	TCP	Iso-tsap	*	ISO-TSAP.
103	TCP	X400	*	ISO Mail.
104	TCP	x400-snd	*	
107	TCP	Rtelnet	Block	Remote Telnet Service.
109	TCP	Pop-2	*	Post Office Protocol - Version 2. See CERT advisory 97-09.
110	TCP	Pop-3	*	Post Office Protocol - Version 3. See CERT advisory 97-09.
111	TCP;UDP	Sunrpc	*	SUN Remote Procedure Call. See CERT advisories 95-17, 94-02, and ASSIST bulletins 95-49, 95-50.
113	TCP	Auth	=	Authentication Service. Don't send ICMP rejection message if blocked. See ASSIST bulletin 95-43.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
115	TCP	sftp	Block	Simple File Transfer Protocol.
117	TCP	Uucp-path	Block	UUCP Path Service. See CERT advisory 92-06.
119	TCP	Nntp	*	Network News Transfer Protocol. Use source and destination address filters if allowed in.
121	TCP	Ercp	*	Encore Expedited Remote Procedure Call.
123	TCP;UDP	ntp	*	Network Time Protocol.
133	TCP	Statsrv	*	Statistics Service. See CERT advisory 97-26 and ASSIST bulletin 96-12.
135	TCP;UDP	Loc-srv	Block	
137	TCP;UDP	Netbios-ns	*	NETBIOS Name Service.
138	TCP;UDP	Netbios-dgm	*	NETBIOS Datagram Service.
139	TCP	Netbios-ssn	*	NETBIOS Session Service.
143	TCP	Imap2, 4	*	Interim Mail Access Protocol v2.
144	TCP	NeWS	*	Block as if X11.
150	TCP	Sgl-net	*	SQL-NET.
153	TCP	Sgmp	*	This was SNMPs predecessor.
161	TCP;UDP	Snmp	Block	Network Time Protocol.
162	TCP;UDP	Snmp trap	Block	Network Time Protocol.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
177	UDP	Xdmcp	Block	X Display Manager Control Protocol.
179	TCP	bgp	=	Border Gateway Protocol.
193	TCP	Srmp	*	Spider Remote Monitoring Protocol.
194	TCP	irc	*	Internet Relay Chat Protocol. See CERT advisory 94-14 and ASSIST bulletin 93-33.
220	TCP	Imap3	*	Interactive Mail Access Protocol v3 See CERT advisory 97-09.
256	TCP;UDP	rap	*	
257	TCP;UDP	set	*	
389	TCP	Ldap	*	
512	TCP	Exec	Block	
512	UDP	biff	Block	Dangerous and buggy service.
513	TCP	Login	Block	See CERT advisories 95-15, 94-09.
513	UDP	who	Block	Nothing legitimate on this port. Alarm it and block.
514	TCP	Shell	Block	
514	UDP	Syslog	*	Can gain access to audit logs. Dangerous See CERT advisory 95-13.
515	TCP	Printer	Block	Line printer spooler. See CERT advisories 97-19, 95-15.
517	UDP	Talk	*	Actual talk protocol uses random TCP ports. See CERT advisory 97-04 and ASSIST bulletin 97-07.
518	UDP	Ntalk	Block	Same as talk.

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
520	UDP	Route	*	Outsiders can gain access to routing tables.
530	TCP	Courier	Block	Experimental.
540	TCP	Uucp	Block	Historically a dangerous service, and mostly obsolete on the Internet. Block. See CERT advisory 92-06.
543	TCP;UDP	Klogin	Block	See CERT advisory 97-06.
550	TCP;UDP	New who	Block	
600	TCP;UDP	Pcserver	Block	ECD Integrated PC board server.
744	TCP;UDP	Flexlm	Block	See CERT advisory 97-01.
749	TCP;UDP	Kerberos- admin	*	
770	TCP;UDP	Cadlock	*	
1025	TCP	Listener	Block	System V Rel 3. If needed, change the listener port.
1105	TCP;UDP	Win6530	*	
1106	TCP;UDP	Win6530	*	
1352	TCP;UDP	Lotusnote	*	Lotus Notes.
1365	TCP;UDP	Adapt-sna	*	Network Software Associates.
1524	TCP	Ingreslock	Block	
1642	TCP;UDP	Isis-am	*	
1645	TCP;UDP	Datametrics	*	

TCP/UDP Port and Service Filtering Guide				
Port	Protocol	Service	Security	Description
1679	TCP;UDP	Darcorp-lm	*	
2000	TCP;UDP	Callbook	Block	
2049	TCP;UDP	nfs	*	NFS server daemon. See CERT advisories 96-09, 94-15, 94-02, 93-15, 92-15, 91-21 and ASSIST bulletin 94-41.
2065	TCP;UDP	Dlsw	*	Data link switch.
2766	TCP	Listen	Block	NLPS server; Also SYS V listener.
2767	TCP;UDP	Ttymon	*	Terminal monitor.
6000-6xxx	TCP	x11	Block	Block the entire range of x11 ports if possible.
6667	TCP	IRC	Block	Internet Relay Chat may or may not be a security risk per se, but some channels attract the sort of network people who send out ICMP Destination Unreachable messages. See CERT advisory 94-14 and ASSIST bulletin 94-33.
12345	TCP	Netbus	Block	
12346	TCP	Netbus	Block	
31337	TCP;UDP	Back orifice	Block	

d. Recommended Permitted Services. The following useful and potentially available services are common among corporate IT providers. These services should be allowed through the router or firewall to permit effective use of the NIPRNET:

1) Outgoing FTP, Passive and Normal

2) Outgoing Telnet

3) Incoming and Outgoing World Wide Web

4) Incoming and Outgoing Secure World Wide Web

5) Incoming and Outgoing Mail

6) Incoming and Outgoing DNS

6. Security of Router Filter Configuration

a. Routers will be located in a secure area with limited access. The Terminal Area Security Officer (TASO) will have ultimate authority to determine who has access to the router, both physically and administratively.

b. All router access shall be password protected, regardless of functionality or lack thereof; such as, console, auxiliary, Teletype (TTY), or network. Passwords will meet the requirements of Tab D paragraph 7. Default vendor passwords and SNMP community names will be changed prior to placing the device on the network.

c. Out-of-band management is the preferred method for accessing a router. In-band management should be limited to emergency situations. The password should be changed immediately after in-band access unless a valid transmission security medium is used throughout the session (such as SSH, Secure Telnet, etc). This applies to all routers, regardless of network.

d. Password encryption will be used to protect the password value in the configuration files

e. Router access privileges will be consistent with the responsibilities of the user. (For example, some users need read access only while others will require write access.)

f. IP alias command should be disabled, if this is an option.

g. Access to sensitive areas of the router (such as, routing tables, access control lists, etc.) shall be permitted only to authorized individuals, as determined by the TASO. These top-level users and their passwords should be recorded and stored in a secure location by someone outside the chain of accountability should one of these privileged users no longer have access requirements. This precludes a single individual from denying authorized users necessary access by not telling them the password or by changing it to something unknown.

h. The appropriate audit-related Remote Monitoring (RMON) functions on the router shall be used in conjunction with an audit repository system.

i. All changes to the configuration of the router will be recorded and audited. The router will be configured to send a Simple Network Management Protocol (SNMP) system message for such occurrence.

j. All routers with SNMP will use an access control list to deny SNMP data to unauthorized users. Default community strings will be changed prior to the device being placed on the network. All SNMP community strings will be protected as passwords.

k. All media will be virus-scanned prior to use on any NETWORK router. Routers will be configured to automatically scan for viruses upon system boot-up, if possible.

7. Policy

a. Network AIS routers will be configured to reject inbound packets from addresses of known likely originators of computer network attack and from addresses that are not allowed.

b. Network AIS routers will be configured according to the NSA/DISA Security Technical Implementation Guide (STIG) for networks (routers).

c. Network AIS routers will be configured to restrict traffic only to known routers within the cognizant theater COCOM architecture and to known and trusted external systems.

d. Network AIS routers will be configured to monitor, audit, and provide alarms for unknown routers attempting to protocol handshake.

e. Network AIS routers and firewalls will be configured to automatically reject all services that are specifically denied. Routers with Simple Network Management Protocol (SNMP) will use an access control to deny SNMP data to unauthorized users.
f. Commanders will maintain a continual review of the various security vulnerability alerts, and recommend additional filtering as considered necessary to remain abreast of current technology and to maintain a viable perimeter defense.

g. All network AIS router access points (regardless of functionality), and router level passwords (privileged and non-privileged) will be configured to enforce password complexity in accordance with this appendix. Vendor-provided passwords and community names will be changed.

h. All network AIS router changes to settings and enhancements will be recorded and audited. Routers will be configured to alarm a Simple Network Management Protocol system for such occurrences.

i. All network AIS routers will be located in secure areas, with physical and administrative security maintained by assigned TASOs.

j. Access to sensitive areas of NETWORKAIS routers will be restricted to authorized personnel.

This page intentionally left blank.

TAB F Firewall Policy

1. Purpose

The purpose of this tab is to establish policy for employment of Firewalls within networks and systems accessing and comprising the deployed network. Waivers to this policy must be submitted through the cognizant COCOM J6.

2. General

a. Typical required firewall functions:

(1) A properly configured firewall provides boundary protection to restrict access to the network.

(2) The firewall automates protection and provides alerts against external network attacks and insider attacks that attempt to penetrate internal, protected enclaves.

b. The primary function of a firewall is access control, allowing and denying network access based upon the security policy of the network or enclave. There are three common types of firewalls:

(1) Packet filtering. A router configured to accept or deny access of packets by examining the source and destination as well as the protocol of the packet. This represents a generic capability that does not account for application behavior.

(2) Stateful inspection. A form of packet filtering that examines a packet's information on several layers of the Open Systems Interconnection (OSI) model to determine whether to deny or permit the packet.

(3) Proxy-based/application gateway. Receives traffic at the Internet Protocol (IP) layer of the OSI model and brings it up to the application layer for inspection by its rule base. A proxy eliminates direct connection to the internal client or server and protects them from the external network. This type of network appliance provides the greatest control and granularity in controlling access to network services.

3. Policy

a. Network users will deploy and configure firewalls to protect all Automated Information System (AIS) networks within their purview. CENTRIXS firewall requirements are different for each Coalition network and will be provided in the respective CONOPS. This approach fully complies with the Department of Defense (DOD) "Defense-in-Depth" approach to Information Assurance (IA), and is establishing technology-specific architectures including enclave boundary protection devices. An enclave is an environment under the control of a single authority through the use of prescribed personal and physical security measures.

Another key to successful IA is the employment of a layered security strategy to reduce vulnerabilities and defend against a wide range of threats.

b. Prior to connectivity to an network AIS, minimum acceptable firewall standards must be in place for the connecting system, and installed behind the theater COMCOM IDS as specified in Tab P of this appendix.

4. Mandatory Settings for Network Ports, Protocols and Services

DOD policy is to support the Joint Task Force – Computer Network Operations (JTF-CNO) Ports, Protocols, and Services (PPS) registration program. This program requires that services, combatant commanders, and agencies register the network ports, protocols and systems that are in use by the organization.

a. Each Service Component (and service elements) is responsible for ensuring that required network PPS to support normal operations are registered and maintained in the PnP database. Registration associates a specific system (such as, JWLI, DMS) with those PnP required to operate.

b. Access to Networks requires commanders to consider JTF-CNO PPS risk category designation when adding or changing systems that will require network interconnectivity. The cognizant theater COCOM J6 must be informed, via service Component, when Unit Commanders accept the risk introduced by a system(s) using high-risk PPS on NIPRNET. The PPS risk category concept is enforceable by DOD policy only to NIPRNET assets at this time. However, to ensure unit commanders maintain total awareness of vulnerability posture, it is recommended that units also monitor SIPRNET systems in a similar fashion, especially those that consistently require the use of high risk (RED) PPS.

(1) The following are established PPS risk category designations. Risk category association is the Assistant Secretary Defense for Command, Control, Communications and Intelligence (ASD C3I) determination based on PPS, Exploitability/Vulnerabilities of PPS; and mitigation efforts.

(2) PPS will be categorized into three groups as a baseline for this annex:

(a) **RED**. Exceptionally vulnerable PPS that will cause significant damage if exploited, or is by nature insecure. This category also includes those legacy PPSs where the functionality is available through a more secure method (eg telnet vs. SSH). PPS designated as Red represents an unacceptably high risk for routine use, due to lack of mitigation strategy. A Red PPS should not be used, but may be allowed when approved by the cognizant DAA for a specific information system under defined conditions. It is emphasized that a category RED PPS is <u>not</u> statically defined as a specific range of ports or protocols, but rather if the PPS can be controlled and/or mitigated to an acceptable level of risk through the use of other technologies and/or policies.

(b) **YELLOW**. Use of PPS in this category includes an acceptable level of risk for routine use when used with required mitigation strategy. A Yellow PPS is not considered acceptable under all implementations within the published standards, but can be brought to an acceptable risk level if required mitigation strategy is implemented and approved by the cognizant DAA for a specific DOD information system.

(c) **GREEN.** A PPS that has been designed or inherently supports robust data/transmission security. To support defense-in-depth strategy, these should also be used under "conditional" circumstances.

(3) Mitigation efforts for some of the vulnerable (high-risk) PPS may include additional constraints placed on the PPS:

(a) Packets can be filtered based upon the source or destination machine IP address. Referred to as "point-to-point", there is a degree of mitigation achieved by limiting the use of the PPS to only those machines that need the service. This mitigation shall normally be used to satisfy *conditional use* requirements if used in conjunction with other mitigation steps. Used alone, this may be defeated by IP spoofing, session hijacking (redirect). Use of this mitigation technique can be bolstered with the use of reverse DNS authentication.

(b) User Identification & Authentication should be used in concert with other mitigation techniques. Many advance firewalls can be configured to use Terminal Access Controller Access Control System (TACACS), Public Key Infrastructure (PKI), or domain authentication services.

(c) Demilitarized Zones (DMZ) or Virtual Private Network (VPN). The use of a DMZ provides a security buffer zone for those machines that routinely provide content/data to users outside the enclave. Units should ensure that DMZ services have a robust recovery process in place. A VPN provides an encrypted channel by which two (or more) enclaves may exchange high-risk PPS. To ensure security of data and services, VPN's should be configured as a *tunnel* (or tunneling) VPN rather than *transport*.

(d) Alternate ports or port redirection may be used in some circumstances. Malicious network scanning commonly defeats this mitigation step, and network configuration overhead is increased. Use of alternate ports requires theater COCOM J6 approval.

5. Category RED PPS

It is network access policy that no new systems that rely on category RED PPS will be accredited. Cognizant theater COCOM DAAs may make case-by-case determination for legacy systems. Component and Unit Commanders, when acting as DAA for a system, possess a responsibility to document residual risk that is introduced when using a system that

relies on high risk PPS for which there is no technical or procedural way to mitigate vulnerabilities (RED) PPS.

6. Proxy Firewall

Implementation of an application layer proxying firewall provides sufficient granularity in the control and mitigation efforts involving PPS. Through stateful inspection and proxying, the risk to PPS may be mitigated to an acceptable residual level in order to support operations.

a. NIPRNET.

The Ports and Services Filtering Table is the network standard for NIPRNET firewall configuration and is located … The table reflects configuration minimums, as well as provides risk level association. Ports with "Cond" identified indicate restricted ports that will be treated as and include a rule that identifies "Deny"; however, Components may specify specific inbound and/or outbound IP addresses, as indicated in the table, that are allowed to use that port for specific purposes. All other IPs shall default as "Deny" for that service port.

b. SIPRNET

(1) The tables reflecting default SIPRNET firewall PPS configuration policy is located at (Note: Need to identify and position this information on a SIPRNET web site similar to the CENTCOM one located at http://recluse.centcom.smil.mil/ccj6/ccj6_c/public/dio/PPS/sipr.htm or under the "Areas - Information Assurance" menus at http://www.tcccfwd.centcom.smil.mil/.)

(2) Network SIPRNET PPS configuration standards. This table reflects configuration minimums, as well as provides risk level association. Ports with "Cond" identified indicate restricted ports that will be treated as and include a rule that identifies "Deny"; however, Components may specify specific inbound and/or outbound IP addresses, as indicated in the table, that are allowed to use that port for specific purposes. All other IPs shall default as "Deny" for that service port.

c. CENTRIXS

Firewall requirements for CENTRIXS differ based on the version of CENTRIXS in use. When firewall usage is required by the CONOPS the required the Ports and Services Filtering Table for CENTRIXS firewall configuration by version and is located at (Note: Need to identify and position this information on a SIPRNET web site similar to the CENTCOM one located at http://recluse.centcom.smil.mil/ccj6/ccj6_c/public/dio/PPS/centrixs.htm and under the "Areas - Information Assurance" menus at http://www.tcccfwd.centcom.smil.mil/.) The table reflects configuration minimums, as well as provides risk level association. Ports with "Cond" identified indicate restricted ports that will be treated as and include a rule that identifies "Deny"; however, Components may specify specific inbound and/or outbound IP

addresses, as indicated in the table, that are allowed to use that port for specific purposes. All other IPs shall default as "Deny" for that service port.

The following table reflects the default network NIPRNET and SIPRNET firewall Internet Control Message Protocol.(ICMP) configuration policy.

ICMP Message Number	**ICMP Message name**	**Configuration Recommendation**
0	Echo Reply	Allow outbound only
3	Destination Unreachable	Allow outbound only
4	Source Quench	Allow both directions
8	Echo Request	Allow outbound only
11	Time exceeded	Allow inbound only
12	Parameter problem	Allow both directions

This page intentionally left blank.

TAB G Remote Administration

1. Purpose

The purpose of this tab is to establish policy for remote workstation/terminal and dial-in access to deployed network Automated Information Systems (AIS) and networks for the purposes of performing administrative actions upon those systems/networks. Waivers to this policy must be submitted through the cognizant theater COCOM J6.

2. Background

a. Remote administration is defined as the performance of system/network administrative actions and functions upon a system, network, or network component from a separate device or terminal linked by a communication medium.

b. The two basic options for managing a system/network are "in-band" and "out-of-band."

(1) In-band management is accomplished by establishing a Network Virtual Terminal Protocol (TELNET) or Secure Shell (SSH) session with the device. Note- Due to security risks associated with TELNET communications, this is the least desirable method of remote administration see paragraph 3.a (following).

(2) Out-of-band management consists of accessing the remote device via a dial up circuit or a directly connected terminal device. With the dial-up method, a modem is attached to the console service port and the administrator connects via a standard phone line. This connection is relatively secure, since connection times are random and the circuit is disconnected when not in use. The most secure out-of-band management is directly connecting a computer or terminal to the console or auxiliary port.

3. Policy

This policy is for all Global Information Grid (GIG) connected devices, regardless of network classification level.

a. Use of Telnet for in-band administration is authorized only for emergency situations to individuals granted prior authorization to do so by the Terminal Area Security Officer (TASO). Once the remote administration is complete the remote administration password must be changed by personnel that can physically access the device.

b. Secure remote administration of all system/network administrative actions and functions are permitted unless prohibited by local policy. Approved methods include National Security Agency (NSA) -approved Virtual Private Network (VPN) technologies and Secure Shell version 2 (SSHv2). Remote administration using services such as TELNET, SSHv1, or a non-approved VPN are not authorized and require the TASO to submit a waiver to the cognizant theater COCOM J6.

c. Audit trails will be reviewed daily when possible, or at a minimum weekly by IA security analysts or System Administrators. Administration may include tasks from the following non-exhaustive list:

- Remotely enable and/or disable command extensions.
- User account/security management (adding and/or deleting users and groups from the global or local user list).
- Changing access privileges to specific resources, such as files or machines.
- Invoke Net commands.
- Check, verify, start or stop services running on an NT or Unix computer.
- Modify existing User properties.
- Establish account policies, including forced log-off after account hours expire.
- Add a new user or delete an existing user.
- Force password changes after approved password duration expires.
- Software distribution, configuration, and version updates.
- Reboot remotely for changes to take effect.
- Troubleshoot software and hardware failures.
- Install automated tasks to perform daily maintenance.
- Capture and filter network traffic.
- Remotely connect to the console when required.

d. The authorizations to perform remote administration under waiver conditions will be revalidated at least once per year by the TASO.

4. Security of Remote Administration Capabilities

a. In-band remote administration will be conducted only when all the following criteria are employed:

(1) Identification and authentication.

(2) Properly encrypted telecommunications for the network device being accessed, to include password encryption.

(3) Restriction to a limited number of authorized Internet protocol (IP) addresses.

(4) Use of Telnet for in-band administration is authorized only for emergency situations to individuals granted prior authorization to do so by the Terminal Area Security Officer (TASO). Telnet sessions must be restricted to specific IP addresses (4 Octets) and by an access control list (ACL). ACL's must not permit networks, or subnets to access the device via Telnet. (Note-Port redirection does not mitigate the non-secure Telnet threat from malicious probes and scanning.)

(5) In-band management will not be used for router management commands.

(6) Passwords will be changed immediately after in-band access if security provisions are not available.

b. Out-of-band management should use the direct connection (AUX/Console) method for communication device management when possible. If direct connection is impractical, the dial-up method is the next best choice.

c. Remote maintenance on a classified system can only be accomplished with encrypted lines, a classified maintenance facility, and appropriately cleared personnel.

d. Dial-in access: Dial-in access will be protected by additional measures, to include:

(1) Dial-back system.

(2) Devices such as caller identification (ID) or the Security Access Control System (SACS) which verify authorized numbers.

(3) Enhanced identification and authentication (I&A) such as smart cards.

(4) Dial-in maintenance on a classified system is only authorized when using NSA-approved encryption and verification of personnel security clearance for maintenance personnel.

e. Lock-outs. Systems must be set to lock out a user ID after three (3) unsuccessful logon attempts. Extremely critical or sensitive systems should be set at two (2) attempts. This is not a cumulative count of unsuccessful attempts. The count will be reset to zero after each successful logon.

f. Time Outs. Systems will be set to terminate or lock out a user session after a period of inactivity, to be determined by the TASO. For classified systems, the timeout must be set to a maximum of 15 minutes unless waived by the Designated Approval Authority (DAA).

g. Dial-in access is restricted to a three-hour connection. After three (3) hours, a mandatory log-off shall be enforced.

5. Additional Special Technical Considerations

a. SMI, MIB, SNMP

The major Components within the TCP/IP based model are Structure of Management Information (SMI), Management Information Base (MIB), and Simple Network Management Protocol (SNMP). The SMI specifies how information about managed objects is to be represented. The MIB contains the definitions and values for the managed objects relevant to a particular network. The information for the MIB component is acquired and updated by a

management agent; a program whose task is to determine and report the information desired by a management program. Continued expansion of a generic MIB has been abandoned in favor of a scheme that allows extensions for specific networking products to be defined as separate nodes. SNMP is the protocol used to represent management information for transmission.

b. Network Management Security Implications of SNMP

(1) SNMP can be a large security risk. Because SNMP can get device information and set device parameters, unauthorized users can cause damage easily. SNMP has three basic commands that can supply information to individuals.

(a) GET. This command is used for MIB variable polling. It is used by the management station to create threshold alarms, provide system settings, and show other device information.

(b) SET. This command is used from the management station for altering a variable's value. It can trigger unintended side effects such as causing the managed device to reset a counter or to reboot.

(c) TRAP. This command is used to set up agents to asynchronously notify the management station of a significant event, such as a change in the availability status of a communication link.

(2) SNMPv1 and SNMPv2 vary slightly in their implementation. SNMPv2 is a super-set of SNMPv1. SNMP messages are constructed into a Protocol Data Unit (PDU). PDUs contain authentication credentials used to apply access control restrictions. The need for authentication is clear: read and write access to some MIB variables may be vital for security, especially those that reveal sensitive information about a system, or cause an action (like a reboot) that can result in a temporary denial of service or hardware destruction.

(3) The original version, SMNPv1, utilizes a trivial authentication mechanism that effectively deems all messages authentic. Each agent knows an alleged secret - essentially a password, known as a community string or name. Both the managing station and the managed station know and share this password. The community name is transmitted in clear text in every PDU making them visible to network eavesdroppers. Unauthorized users can use these community names to forge their own messages or replay old ones at will.

(4) SNMPv2 supports several viable security mechanisms. Through cryptographic means, the new SNMPv2 message formats provide integrity, sender authentication, and confidentiality services where they are needed.

(5) To avoid possible attacks, TASOs shall institute the following procedures:

(a) Use digital signatures or encryption, if available, on the devices (such as, devices supporting SNMPv2).

(b) Most systems default to a community name of "public". Change the community name to something that is not easily guessed. Protect it just as you would any password.

(c) Upgrade to SNMPv2 as soon as possible.

(d) Turn off trap-authentication at your routers. This will aid in preventing intruders from using trap messages to discover community strings.
(e) Use the privileged/non-privileged modes of devices that allow such services, especially routers. Use different community names for read-only access and read/write access.

(f) Establish a list of specific IP addresses that are allowed to send messages to the device.

(g) Setup alarms within the managed network's framework. These should include as a minimum the following:

1. Integrity Violations, indicating that network contents or objects have been illegally modified, deleted, or added.

2. Operational Violations, indicating that a desired object or service could not be used.

3. Physical Violations, indicating that a physical part of the network (such as a cable) has been damaged or modified without authorization.

4. Security-mechanism Violation, indicating that the network's security system has been compromised or breached.

5. Time-domain Violation, indicating that an event has happened outside its allowed or typical time slot.

(h) Categorize alarms by severity using the following guidelines*:*

1. Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore a service that has been lost completely.

2. A major alarm indicates that steps must be taken as soon as possible, because the affected service has degraded drastically and is in danger of being lost completely.

3. A minor alarm indicates a problem that does not yet affect service, but that may do so if the problem is not corrected.

4. A warning alarm is used to signal a potential problem that may affect service.

5. An indeterminate alarm is one that requires human intervention to decide its severity.

c. SIPRNET users, desiring classified access, must dial-in to a Communications Server with an approved router that is running Terminal Access Controller Access Control System Plus (TACACS+). The TACACS+ will interact through an approved secure access connection.

TAB H IA Vulnerability Alert (IAVA) Policy

1. Purpose

The purpose of this tab is to establish policy for compliance and reporting of Information Assurance Vulnerability Alerts (IAVA). Waivers to this policy must be submitted through the cognizant theater COCOM J6.

2. Background

a. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I) tasked the Defense Information Systems Agency (DISA), as the Departments executive agent, to develop an IAVA process. This process is designed to provide a measure of risk avoidance within the overall Information Assurance risk management framework.

b. Component Headquarters are tasked as executive agents for ensuring IAVA compliance for those service elements operating within the NETWORK. Compliance will be dual reported; through the operational (deployed) Joint Network Operations (NETOPS) reporting chain, and back through applicable administrative service channels.

c. DAAs of the Joint Force headquarters and the Component Commands will make final IAVA related risk management decisions and assign waivers for all systems/assets under their purview. Any waiver of IAVA requirements or delay in compliance must be reported as part of the compliance reporting.

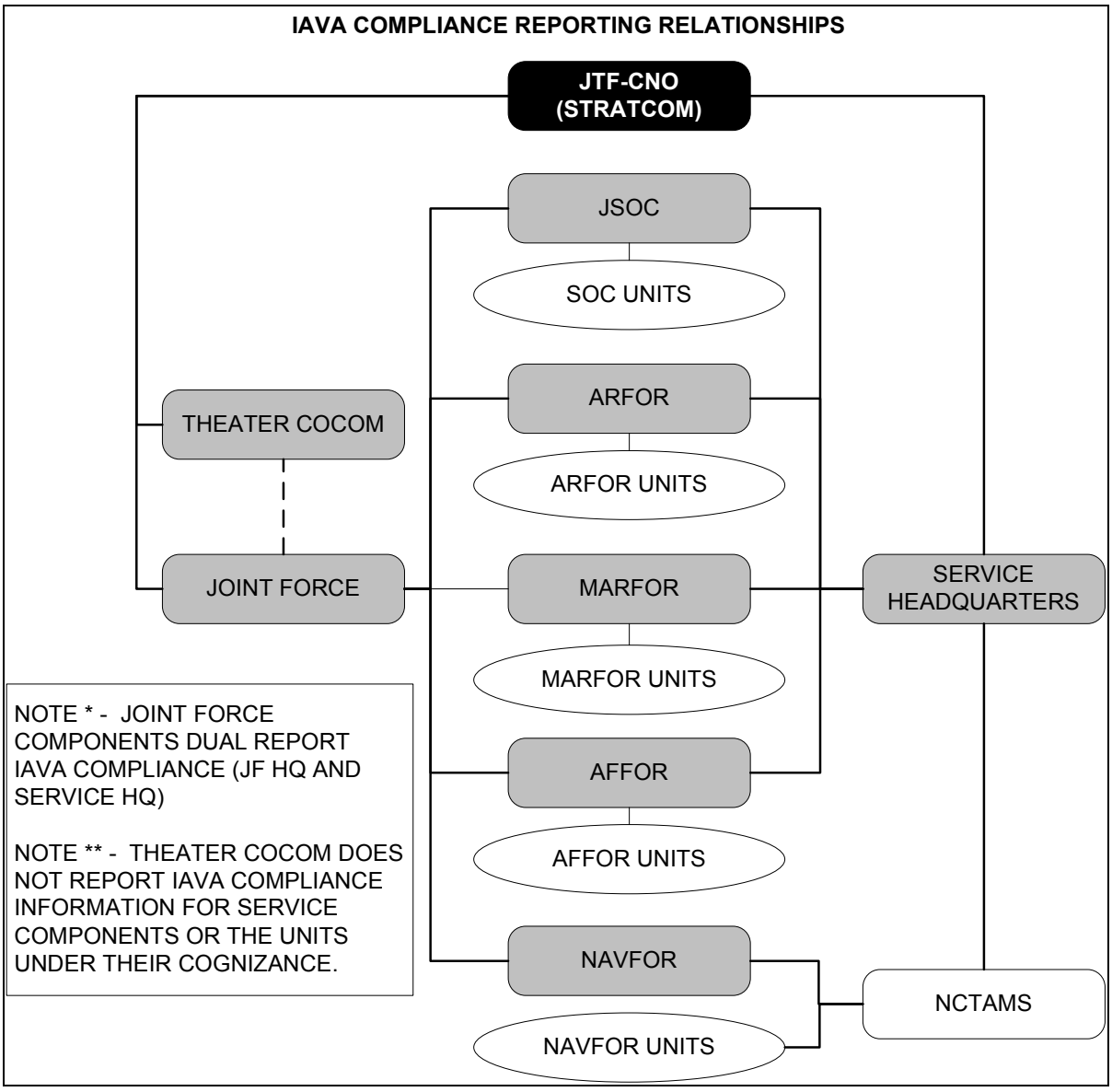
d. When a vulnerability notice is published by the Department of Defense Computer Emergency Response Team (DOD-CERT), users will be directed to access the DOD CERT Web-site to obtain detailed information. Web-site URLs are:

(1) http://199.211.123.12 Unclassified (also Sensitive but Unclassified) IAVA database.

(2) http://www.cert.smil.mil/iava Classified IAVA Database.

3. Policy

a. Joint Force headquarters and Component Commands are responsible for complying with IAVAs and reporting compliance and/or waiver status to cognizant theater COCOM J6 in addition to prescribed service specific requirements. Theater COCOMs will not intercede in service reporting requirements, nor reflect service element compliance as part of their reporting metrics. Lateral reporting by the service Components is necessary for JTF and COCOM ability to maintain situational awareness of potential NETWORK vulnerabilities.



b. Deployed Joint Force headquarters, Joint Special Operations Command headquarters, and service components headquarters will establish local NETOPS control centers to serve as focal points for handling incidents and network management at the lowest level.

c. Service component headquarters are also required to simultaneously report to their service computer emergency response team (CERT)/Computer Incident Response team (CIRT).

d. Deployed Joint Force headquarters, Joint Special Operations Command headquarters, and service components headquarters will establish a unique billets within their NETOPS organizations to handle IAVA responsibilities. These billets should have published organizational email accounts (NIPRNET/SIPRNET/CENTRIXSs), point of contact phone numbers and plain language address (PLA) information. A command/unit point of contact

needs to be available 24x7. The IAVA POC must have sufficient training and standing operating procedures to ensure proper response to critical computer incidents/events.

e. Component NETOPS control centers are responsible for those units OPCON to them. They will establish procedures to capture and report compliance statistics subordinate commands/units.

f. Component NETOPS control centers will establish a method of displaying compliance status via their respective SIPRNET web pages. The minimum content of this 'IAVA Compliance' page will include a table that reflects:

(1) Component & subordinate unit name(s)

(2) IAVA number (such as IAVA-A-2003-002)

(3) Compliance indicator: Can be expressed as a numerical percent (patched/affected=%compliant). The use of colors and/or symbols may also be used as long as symbology or color schema is parallel to JTF-CND and DISA accepted standards.

(4) Post a date-time-group on the page to indicate when the content was last updated.

This page intentionally left blank.

TAB I to Foreign National Access to NIPRNET at Component Sites Within The Joint AOR

1. Purpose

The purpose of this tab is to establish policy for NIPRNET account establishment for Foreign Nationals to NETWORK connected Automated Information Systems (AIS). Waivers to this policy must be submitted through the cognizant theater COCOM J6.

2. Background

a. There are instances when a deployed military mission will have an operational requirement for friendly foreign national personnel assigned to US Forces to have access to portions of the U.S. NIPRNET. Unrestricted NIPRNET access for friendly foreign national personnel will not be granted. However, it is critical that these allies be permitted access to the NIPRNET in order to function in their roles to support Joint Forces and/or Component Commands. Component DAAs are responsible for reviewing applications of foreign nationals to ensure a valid requirement exists prior to authorizing the any network access. The intent of this policy is to prevent a requirement to set up separate internet access networks for assigned foreign nationals.

b. Policy for providing Foreign Nationals access to NIPRNET must follow DOD Dir 8500.1 and DOD Dir 8500.2. General NETWORKNETEWORK provided NIPRNET access for Foreign Nationals **must be validated and approved by the Joint Chiefs of Staff**, via request of the cognizant theater COCOM. (An example might be to request Foreign National access during a specific Operation or Exercise.)

3. Policy

a. The following procedures apply when granting NIPRNET access to Foreign Nationals.

(1) Joint Force/Component DAA approval of individual justification by name.

(2) Foreign Nationals complete security awareness/training annually. (Exhibit (1))

(3) Foreign National signs NIPRNET account user agreement.

(4) Establish NIPRNET account using specific naming convention: USERNAME.COUNTRYCODE@COGNIZANT COCOM.MIL**.** The country code will be the 2 letter code from FIPS 10-4 or ISO Standard 3166.

(5) Assign the user account to a specific NIPRNET terminal with a static IP address specifically designated for foreign access. User account will have unique user name and password.

(6) Components will maintain a listing of static IP addresses that are serving their foreign nationals.

(7) Foreign National user access to NIPRNET will be limited to only those sites the foreign national individual has a need to know to access. Method of limiting access is at the discretion of the local DAA, as long as intent is met. It is recommends that Reverse DNS Look Up be disabled on the specific IP address to meet this requirement.

(8) Foreign National access to web sites falling within the purview of the cognizant theater COCOM may be allowed on a need-to-know basis. Other restricted web sites will be denied unless approved by the controlling authority over those web sites. Publicly available web sites are permitted as long as they follow acceptable standards as indicated in the user statement below.

b. Remote Dial-up Access. Foreign National NIPRNET access via remote dial up must be done adhering to the following:

(1) A specific remote access services (RAS) server must be utilized for Foreign National access only.

(2) The Foreign National will only have the dial in number for the Foreign National RAS Server.

(3) Assign an IP range to be utilized on the Foreign National RAS Server and provide to the cognizant theater COCOM J6.

c. The following information must be provided to cognizant theater COCOM J6 when a Foreign National is given access to the NIPRNET:

(1) User Name.

(2) Country or Nationality.

(3) US Sponsor/Activity.

(4) IP address.

(5) Justification.

d. The completed Statement of Understanding Form will be retained locally.

Exhibits

1-FOREIGN NATIONAL NIPRNET ACCESS STATEMENT OF UNDERSTANDING

EXHIBIT 1 to TAB I Foreign National NIPRNET Access Statement Of Understanding

FOREIGN NATIONAL ACCESS TO NIPRNET AT DEPLOYED SITES - RECORD OF TRAINING AND STATEMENT OF UNDERSTANDING

1. Official Use and Authorized Purposes

a. NETWORKaccess AIS users fall under DOD 5500.7-R, Joint Ethics Regulation (JER), Section 2-301 (Change 2) dated 22 March 1996. The JER directs that the use of government communications systems and equipment (including computers, electronic mail, and Internet systems) "shall be for official use and authorized purposes only."

(1) _____ Official Use. 'Official use' refers to users that directly further the interests of DOD and the duties prescribed for the individual position.

(2) _____ Authorized Purposes. 'Authorized purposes' refers to personal use within specified limits as permitted by an appropriate level Supervisor.

b. Before authorizing personal use, a supervisor must determine that the use:

(1) _____ Does not adversely affect the performance of official duties by the DOD employee or the DOD employee's organization.

(2) _____ Is of reasonable duration and frequency and occurs during an employee's personal time (before/after duty hours, during lunch, or authorized breaks).

(3) _____ Serves a legitimate government interest.

(4) _____ Is not used for purposes that adversely reflect upon the US Military, DOD and the Federal Government.

(5) _____ Does not overburden Federal Government computing resources, communications systems, or result in added costs to the Government.

d. Authorized purposes for limited personal use include the following e-mail or web-based activities:

(1) _____ E-mailing short messages to a relatives or colleagues.

(2) _____ Receiving e-mail (as long as comparable receipt would be acceptable via telephone, and is no more disruptive than a telephone call).

(3) _____ Making a medical, dental, auto repair, or similar appointment.

(4) _____ Improve professional or personal skills as part of a formal academic, military or civilian professional development program (when approved by an immediate supervisor).

(5) _____ Serves a legitimate public interest such as enhancing professional skills, improving morale of personnel stationed away from home for extended periods.

2. System Security

a. _____ I understand that all floppy disks, tape drives and removable storage media must be properly labeled to their perspective security classification.

b. _____ I understand that all the data to be processed on DOD computer assets is for official or authorized use only.

c. _____ Removable memory devices from a SECRET computer cannot be connected to an UNCLASSIFIED computer. (If a SECRET memory device is connected to an UNCLASSIFIED computer, that computer becomes SECRET.)

d. _____ Any UNCLASSIFIED removable memory device connected to a SECRET computer must be write protected. (If not, the UNCLASSIFIED memory device becomes SECRET.)

e. _____ UNCLASSIFIED DOD computers will be used to obtain or exchange information to support DOD sanctioned missions.

f. _____ UNCLASSIFIED DOD computers with internet access can be used to obtain or exchange information that enhances the professional skills of DOD personnel/employees and/or benefits the US Government.

g. _____ UNCLASSIFIED USCENTCOM computers with Internet capabilities can be used to improve professional or personal skills as part of a formal academic education or military or civilian professional development program (when approved by an immediate supervisor).

3. Prohibited Use of Internet Services

a. The use of Internet services in the following types of activities is specifically prohibited:

(1) _____ Activities with purposes for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, or sales of personal property.

(2) _____ Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment.

(3) _____ Fundraising activities for commercial, personal, or charitable purposes. (Official morale, welfare, recreation, officer, and enlisted aid activities are authorized.)

(4) _____ Using NETWORK access AIS networks as a staging ground or platform to gain unauthorized access to other systems.

(5) _____ Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

(6) _____ Accessing, creating, downloading, viewing, storing, copying, processing, displaying, or transmitting sexually oriented or racist materials.

(7) _____ Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities, or activities otherwise prohibited.

(8) _____ Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

(9) _____ Posting DOD information to external newsgroups, bulletin boards, or other public forums without authority.

(10) _____ Accessing sites with continuous data streams (such as, audio, or video such as Pointcast).

(11) _____ Accessing sites known for hacker attacks or hacker activity.

(12) _____ Accessing or participating in Internet Relay Chat sessions.

(13) _____ Downloading shareware/freeware software or executable programs (such as, .EXE, .COM, .BAT, or script.INA files).

(14) _____ Participating in “spamming,” that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

(15) _____ Participating in “letter bombing”; that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient’s use of e-mail.

(16) _____ Broadcasting unsubstantiated virus warnings from other than official DOD sources.

(17) _____ Opening e-mail attachments from unknown or questionable sources or opening attachments from such sources without downloading to disk and virus scanning.

(18) _____ Storing, processing, or distributing classified, proprietary, or other sensitive or For Official Use Only (FOUO) information on a computer or network not explicitly approved for such processing, storage, or distribution.

(19) _____ Using another person's account/identity without previously obtaining explicit permission (such as, forging e-mail).

(20) _____ Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.

(21) _____ Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.

(22) _____ Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyrights, trade secret, or license agreement.

(23) _____ Allowing any unauthorized person to access a USCENTCOM or DOD-owned system.

(24) _____ Modifying or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

b. _____ Prohibited uses of the Internet can result in administrative, judicial or non-judicial punishment in accordance with federal law, the Uniform Code of Military Justice and civilian employee regulations.

4. Monitoring. Each AIS in USCENTCOM shall be subject to a minimal audit as described below:

a. _____ Use of such systems serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. Monitoring can include accessing files stored both on internal and removable storage media of any type used with the system.

b. _____ Use of such systems is not anonymous. For each use of the Internet, the name and computer address of the employee user can be recorded, as well as the locations searched.

c. _____ Most Government communications systems are not secure. Employees shall not transmit classified information over any communication system unless approved security procedures and practices are used (such as, encryption, secure networks/workstations).

d. _____ Employees shall not disclose communications systems access data (such as passwords) to anyone, unless such disclosure is authorized.

e. _____ Employees shall use extreme care when transmitting sensitive information or other valued data. Information transmitted over an open network, such as e-mail, the Internet, telephone or fax, is accessible to anyone else on the network. Information transmitted through the Internet or by e-mail is accessible to anyone in the chain of delivery, and may be re-sent to others by anyone in the chain.

f. _____ Electronically transmitted information, including e-mail, can become part of official government records, which may be released under the Freedom of Information Act.

g. _____ In order to ensure that such authorized personal use does not adversely affect the performance of official duties, personnel may only go online when needed and must immediately disconnect (close their browser) when they are finished. Users must terminate and log off on completion of their business in order to share resources in multi-user environments. Do not leave Internet connections running throughout the day. Remote dial-in access may only be used for official use (such as, mission-related dial-in from home or TDY location). Personal use of the dial-in capability is prohibited.

h. _____ Periodic reviews of the adequacy of the safeguards for operational, accredited AIS shall be conducted.

i. _____ There will be an audit trail providing a documented history of AIS use to ensure that each person having access to an AIS may be held accountable for his or her actions on the AIS.

j. _____ The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

5. I certify that I have been trained on the above topics and understand the contents of the material that has been covered.

_____	_____	_____
Printed Name	Signature	Date

_____
Command / Unit /Section

This document expires 1 year from the date indicated above. Access beyond this date requires the training be redone and a new document signed. Failure to complete this mandatory training will require that access be terminated until the training is completed.

TAB J CENTRIX Security

1. Purpose

CENTRIXS is a standing, global enterprise network allowing U.S. and coalition nations and their forces to securely share operational and intelligence information in support of combined planning, unity of effort, and decision making in multinational operations. The purpose of this Tab is to establish general policy for use of all versions of the Combined Enterprise Regional Information Exchange System (CENTRIXS).

2. Background

(a) Combatant Commanders (COCOMs) assemble dynamically changing coalitions in response to mission requirements. Command and control networks to support these coalitions need to be flexible and dynamic in order to respond to the commander's mission needs.

(b) National policy dictates what information can be shared with particular coalition partner nations involved in specific operations. Under normal circumstances, coalition information sharing will include all information that commanders need to plan and execute operations and to protect the forces in the area of responsibility (AOR). It should be noted that the COCOM Commander has broad authority for the emergency release of information that affect U.S. and foreign forces within his AOR.

(c) U.S. forces are accustomed to using U.S.-only networks for command, control, communications, computer systems, intelligence, and reconnaissance (C4ISR) and logistics, to plan, train, prepare for, and execute military operations. When faced with the requirement to interoperate with coalition forces, COCOMs often resort to ad hoc methods to exchange information with foreign partner forces. As the scope and the participation of foreign nations increase in importance, commanders require solutions that allow them to seamlessly interoperate with their coalition partners. The commander may decide to conduct his operations on a coalition network, rather than on a U.S. network. This approach supports coalition interoperability, mission accomplishment, and protection of the coalition forces engaged.

(d) Commanders often find themselves isolated from some of the information to which they and their forces are normally accustomed to accessing via a U.S.-only network when working within the constraints of a coalition network. Technical and procedural provisions are have been developed to facilitate the transfer of critical information using guarding technology for finished information products, some databases, real time data, limited email, and limited situational awareness displays. Often though, there is still a requirement to have material reviewed by a Foreign Disclosure Officer (FDO) or representative prior to releasing information to a coalition network.

(e) Commanders may have to use more than one coalition network due to the limits imposed by different applications of security/disclosure policy towards different coalition partners.

Individual CENTRIXS networks operate at an assigned security classification level based on information exchange requirements and the coalition membership.

Operational Environment. Physical operating environments may vary with each CENTRIXS implementation. The following is a listing of general environmental characteristics.

(a) Coalition partners will be responsible for acquiring the baseline COTS hardware and software. The National Security Agency (NSA) approved releasable cryptographic equipment will be provided to the member nations by the COCOM. The J6 will establish the minimum acceptable hardware and software configurations for CENTRIXS workstations that coalition nations will need to obtain and assist, where possible. Coalition nation fiscal constraints and technological capabilities will determine each nation's ultimate equipment end state (such as, numbers and locations of workstations).

(b) Coalition nations will use indigenous communications infrastructure to connect national facilities with CENTRIXS workstations to an appropriate U.S. controlled server gateway.

(c) Coalition partners will execute the required Memorandum of Agreement (MOA) for information sharing and make the necessary arrangements to gain access to the CENTRIXS network. Each nation will work with the COCOM Command, Control, Communications, and Computers Directorate (J6) and appropriate forward Service component to plan and implement connections to the designated gateway servers.

(d) Environmental Constraints.

(1) Non-Disclosure Policy: The release of classified military intelligence is strictly controlled and must be accomplished in accordance with established standards. Combatant Command Regulations on Disclosure Of U.S. Classified Military Information To Foreign Governments and International Organizations establishes the command's specific foreign disclosure guidance and is based on *National Disclosure Policy Manual (NDP-1),* dated 2 Dec 2003. Until viable multilevel security technology is available, CENTRIXS bilateral or Community of Interest (COI) information sharing networks will be physically separate from the other networks to prevent inadvertent release of the information to unauthorized recipients.

(2) Culture: CENTRIXS is designed to allow users the ability to post intelligence and operational information for all participants to access. Information sharing agreements with AOR countries are often mostly one way. Although some AOR countries provide information, the information provided is not to the same level that the COCOM provides to them. The implementation of CENTRIXS is intended to promote the sharing.

(3) Training: Many individuals from coalition nations have little to no computer experience or knowledge. Initial training for these individuals must begin with basic computer operation. Limited computer knowledge could diminish the usefulness of

CENTRIXS to these countries and create a situation where U.S. personnel either are forced to conduct training or revert to hardcopy information dissemination.

3. Policy

a. COCOMs have an operational need for coalition information-sharing environments where information is shared at the appropriate security levels with partner nations and their forces. This environment is available in CENTRIXS. It supports the processing, storing, and transmission of releasable information from pre-hostilities through post-combat operational planning and execution. Only participants of the coalition operation are allowed access within the coalition information-sharing environment, which also has the ability to share information with other systems as required.

b. CENTRIXS access is granted for authorized use only. Such use will be monitored to ensure protection of networks and information. All CENTRIXS users are subject to unannounced computer inspections.

4. Usage

CENTRIXS users, managers, administrators and Terminal Area Security Officers (TASO) shall abide by the same requirements and responsibilities outlined in this appendix for use, management, administration and security of SIPRNET. This includes e-mail use, general use, marking and destruction, annual training, user agreements, incident reporting, monitoring, supervision, workstation locking, password security, and all other requirements and provisions within this appendix.

CENTRIXS Warning Banner. The standard Warning Banner will be modified as indicated below:

THIS IS A CENTRIXS COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR COALITION BUSINESS. CENTRIX COMPUTER SYSTEMS MAY BE MONITORED BY AUTHORIZED PERSONNEL TO ENSURE THAT THEIR USE IS FOR AUTHORIZED PURPOSES, TO INCLUDE MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED.
USE OF THIS CENTRIX COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

This page intentionally left blank.

TAB K Coalition Access to CENTRIX at Component Sites Within The AOR

1. Purpose

The purpose of this tab is to establish general policy for granting coalition personnel (Non-US) access to the Combined Enterprise Regional Information Exchange System (CENTRIXS) located within a deployed US headquarters or control center site..

2. Background

Combatant Commanders have operational requirements for sharing information with Coalition personnel physically located at deployed US headquarters and/or operation centers within a specific AOR. Unrestricted access for Coalition personnel will not be granted; however, it is critical that these partners be permitted access to CENTRIXS in order to function in assigned liaison or support roles. Component DAAs are responsible for validating CENTRIXS access lists to ensure a valid requirement exists prior to authorizing Coalition personnel (Non-US) CENTRIXS access.

3. Policy

a. CENTRIXS networks function in a "System High" mode-of-operation. Under this mode-of-operation, all authorized network users are granted clearance and access for all information processed, stored, or transmitted, on the network. They may not have the need-to-know for all such information.

b. The following procedures apply when granting CENTRIXS access to Coalition partners.

(1) Foreign Nationals complete security awareness/training annually. (Tab A)

(2) Foreign National signs CENTRIXS account user agreement. This agreement will be based entirely on the form provided in Annex H of this appendix modified for Foreign CENTRIXS access.

(3) Establish CENTRIXS account using specific naming convention: domain.command.network.cmil.mil.USERNAME.COUNTRYCODE@domain.command.network.cmil.milCENTRIXS.MIL. The country code will be the 2 letter code from FIPS 10-4 or ISO Standard 3166.

(4) Assign the user account to a specific CENTRIXS terminal with a static IP address.

(5) Components will maintain a listing of static IP addresses that are serving their foreign nationals.

(6) Disable Reverse DNS Look up on the specific IP address.

c. The following information must be provided to the cognizant COCOM J6 when a Foreign National is given access to the CENTRIXS:

- User Name
- Country or Nationality
- US Sponsor/Activity
- IP address
- Justification

Completed 'Record of Training and Statements of Understanding' Forms will be retained locally.

d. Personnel Security. All Coalition personnel afforded unescorted access to areas containing CENTRIXS AIS must be cleared for the highest classification level processed on the system or openly contained in the area and have the appropriate need-to-know.

EXHIBIT 1 TO TAB K Coalition Partner CENTRIXS Access Statement of Understanding

COALITION PERSONNEL (NON-US) ACCESS TO CENTRIX AT DEPLOYED SITES - RECORD OF TRAINING AND STATEMENT OF UNDERSTANDING

1. Official Use and Authorized Purposes

a. Non-US Coalition users of CENTRIXS are required to operate within these guidelines.

(1) _____ Official Use. 'Official use' refers to users that directly further the interests of DOD and the duties prescribed for the individual position.

(2) _____ Authorized Purposes. 'Authorized purposes' refers to personal use within specified limits as permitted by an appropriate level Supervisor.

2. System Security

a. _____ I understand that all floppy disks, tape drives and removable storage media must be properly labeled to their perspective security classification.

b. _____ I understand that all the data to be processed on CENTRIXS computer assets is for official or authorized use only.

c. _____ Removable memory devices from a US SECRET REL XXXX computer cannot be connected to an UNCLASSIFIED computer. (If a US SECRET REL XXXX memory device is connected to an UNCLASSIFIED computer, that computer becomes US SECRET REL XXXX.)

d. _____ Any UNCLASSIFIED removable memory device connected to a SECRET computer must be write protected. (If not, the UNCLASSIFIED memory device becomes SECRET.)

3. Prohibited Use of CENTRIXS Services

a. The use of CENTRIXS services in the following types of activities is specifically prohibited:

(1) _____ Activities with purposes for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, or sales of personal property.

(2) _____ Soliciting business, advertising, or engaging in other selling activities in support of private business enterprises or outside employment.

(3) _____ Fundraising activities for commercial, personal, or charitable purposes. (Official morale, welfare, recreation, officer, and enlisted aid activities are authorized.)

(4) _____ Using NETWORK access AIS networks as a staging ground or platform to gain unauthorized access to other systems.

(5) _____ Creating, copying, or transmitting chain letters or other unauthorized mailings regardless of the subject matter.

(6) _____ Accessing, creating, downloading, viewing, storing, copying, processing, displaying, or transmitting sexually oriented or racist materials.

(7) _____ Accessing, creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities, or activities otherwise prohibited.

(8) _____ Endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

(9) _____ Posting CENTRIXS information to external newsgroups, bulletin boards, or other public forums without authority.

(10) _____ Downloading shareware/freeware software or executable programs (such as, .EXE, .COM, .BAT, or script.INA files).

(11) _____ Participating in “spamming,” that is, exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to provide widespread distribution of unsolicited e-mail.

(12) _____ Participating in “letter bombing”; that is, sending the same e-mail repeatedly to one or more recipients to interfere with the recipient’s use of e-mail.

(13) _____ Broadcasting unsubstantiated virus warnings.

(14) _____ Opening e-mail attachments from unknown or questionable sources or opening attachments from such sources without downloading to disk and virus scanning.

(15) _____ Storing, processing, or distributing classified, proprietary, or other sensitive or For Official Use Only (FOUO) information on a computer or network not explicitly approved for such processing, storage, or distribution.

(16) _____ Using another person's account/identity without previously obtaining explicit permission (such as, forging e-mail).

(17) _____ Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.

(18) _____ Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.

(19) _____ Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyrights, trade secret, or license agreement.

(20) _____ Allowing any unauthorized person to access a USCENTCOM or DOD-owned system.

(21) _____ Modifying or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

b. _____ Prohibited uses of the CENTRIXS can result revocation of system access and referral to appropriate command authority.

4. Monitoring. Each AIS in USCENTCOM shall be subject to a minimal audit as described below:

a. _____ Use of such systems serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized. Monitoring can include accessing files stored both on internal and removable storage media of any type used with the system.

b. _____ Use of such systems is not anonymous. For each use of the CENTRIXS, the name and computer address of the employee user can be recorded, as well as the locations searched.

c. _____ Most Government communications systems are not secure. Employees shall not transmit classified information over any communication system unless approved security procedures and practices are used (such as, encryption, secure networks/workstations).

d. _____ Employees shall not disclose communications systems access data (such as passwords) to anyone, unless such disclosure is authorized.

e. _____ Employees shall use extreme care when transmitting sensitive information or other valued data. Information transmitted over an open network, such as e-mail, the CENTRIXS telephone or fax, is accessible to anyone else on the network. Information transmitted through the CENTRIXS is accessible to anyone in the chain of delivery, and may be re-sent to others by anyone in the chain.

f. _____ Electronically transmitted information, including e-mail, can become part of official government records.

g. _____ In order to ensure that such authorized personal use does not adversely affect the performance of official duties, personnel may only go online when needed and must immediately disconnect (close their browser) when they are finished. Users must terminate and log off on completion of their business in order to share resources in multi-user environments. Personal use of the dial-in capability is prohibited.

h. _____ Periodic reviews of the adequacy of the safeguards for operational, accredited CENTRIX AIS shall be conducted.

i. _____ There will be an audit trail providing a documented history of AIS use to ensure that each person having access to an AIS may be held accountable for his or her actions on the AIS.

j. _____ The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

5. I certify that I have been trained on the above topics and understand the contents of the material that has been covered.

_____	_____	_____
Printed Name	Signature	Date

_____
Command / Unit /Section

This document expires 1 year from the date indicated above. Access beyond this date requires the training be redone and a new document signed. Failure to complete this mandatory training will require that access be terminated until the training is completed.

TAB M Wireless Access

1. Purpose

This tab provides guidance to users accessing CLASSIFIED and/or UNCLASSIFIED data networks through the NETWORK on the usage of wireless networking technologies. For the purpose of this tab, wireless networking technology refers to those devices that operate in the non-licensed (note that some countries may place additional restrictions on this type of communication) radio spectrum to provide a short-range communications medium between computer and networking devices. This includes wireless computer networks, peer-to-peer wireless connections, Personal Digital Assistants (PDA), phones with wireless network access and any other device utilizing 'wireless' technology. The technology is equally appealing to network administrators and users because it is relatively easy to implement and is convenient to end-users. Wireless technology is often used commercially to create independent wireless local area networks (WLAN) or extensions to existing 'wired' local area networks (LAN). Wireless networking poses a significant risk to government information systems and data if not properly implemented.

2. Policy

a. Wireless connections **will not** be used to tie into NETWORKextended data networks except in extreme cases where wired implementation is not possible. All wireless network applications require prior approval of the Cognizant COCOM J6 before being implemented. Approval will not be granted for convenience or because equipment was in use prior to arrival in theater.

b. **All** wireless implementations must comply with the requirements of the Wireless Security Technical Implementation Guide (STIG) created and maintained by DISA Field Security Operations. STIGs are available at: https://iase.disa.mil/documentlib.html#miscellaneous) or (http://cassie.iiie.disa.smil.mil/techguid/documentlib.html#miscellaneous.)

c. Wireless implementations will be clearly indicated on all accreditation documentation (see paragraph 3) and will include COCOM J6 authorization. All wireless frequency usage must be part the approved frequencies allowed by the host nation and follow all applicable agreements and laws.

3. Minimum Requirements

a. Classified Networks

(1) Under no circumstances shall wireless technologies/devices be used for storing, processing, and/or transmitting CLASSIFIED information without written consent of the cognizant Designated Approving Authority (DAA) and approval of the cognizant COCOM J6.

(2) Only assured (encrypted) channels employing NSA-approved, Type-1 end-to-end encryption, shall be used to transmit classified information.

(3) Wireless devices that store, process, and/or transmit CLASSIFIED information shall be handled with the same care that applies to information at that classification levels.

(4) Wireless devices that store, process, and/or transmit CLASSIFIED information, over a network, should use the DOD Common Access Card (CAC) for Identification and Authentication (I&A).

(5) Use of wireless PDAs with classified data is not authorized.

b. Unclassified Networks

(1) Wireless devices that store, process, and/or transmit UNCLASSIFIED information shall only be used over an assured channel having Federal Information Processing Standards (FIPS) 140-1 Overall Level 1 or better, and when products become available, 140-2 Overall Level 1 or better encryption.

(2) The assured channel encryption shall extend from the wireless device up to the premise router into the wired UNCLASSIFIED DOD network.

(3) Encryption implemented over assured channels shall be FIPS 140-1/2 Triple-DES, 128 bit key length, or better, or other Type-2 or Type-1 encryption endorsed in writing by NSA for use with wireless networks.

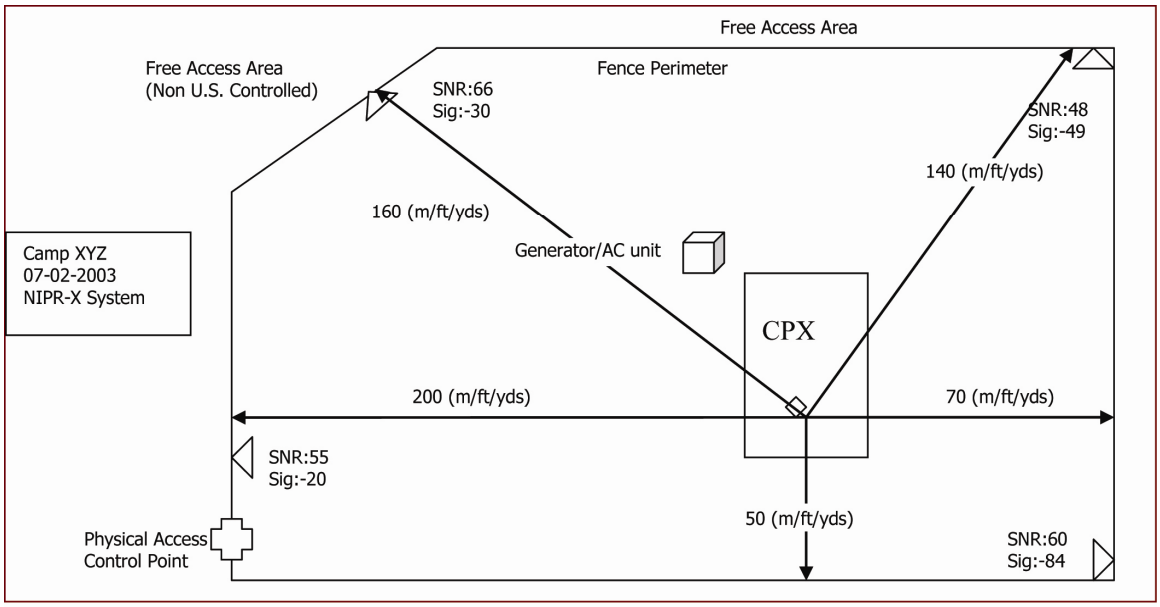
(4) Wireless devices that store, process, and/or transmit UNCLASSIFIED information, over a network, shall use the DOD Public Key Infrastructure (PKI) and the DOD Common Access Card (CAC) for Identification and Authentication (I&A), whenever possible.

(5) The local DAA shall govern the use of wireless devices in areas where classified processing takes place, areas where there are no classified devices but are formally accredited as “open storage” or “closed storage” areas where classified discussions are likely to take place but are not accredited at any level other than unclassified processing, and meeting rooms and conference facilities.

Wireless devices shall not be connected to DOD systems without the approval of the local DAA. DOD-controlled wireless devices shall not be connected to non-DOD systems without the approval of the local DAA and approval of the cognizant COCOM J6. Non-DOD wireless devices shall not be connected to DOD information systems under any circumstances. Devices that have DAA approval shall have readily visible labels attached to them.

Wireless devices/technologies shall be addressed in the overall security architecture when conducting the risk assessment in compliance with the DOD Information Technology

Security Certification and Accreditation Process (DITSCAP) process. An addendum to the required DITSCAP Certification and Accreditation (C&A) documents will include an informal site survey, based on the Concept of Operations (CONOPS) of wireless access point(s) and the generic field of connectivity. This following diagram is an example of the required basic top view of a facility requesting to use a wireless access point. It must include annotations of U.S. controlled perimeters, site boundaries and accurately measured distances between the access point and perimeter. The intent of requiring such detail in the diagram is to establish the extent of the surrounding space under direct U.S. control. Certification and accreditation of networks that include wireless segments shall include in the Systems Access Authorization (SAA) and System Security Authorization Agreement (SSAA), a logical network diagram clearly showing Wireless Access Point (WAP) connectivity. This shall be a separate diagram from overall network topology diagrams, which will also include an annotation of wireless connections. Diagrams should also document Signal-To-Noise (SNR) and/or Signal Strength (expressed as Dbm) at perimeter points. An example is:



Implementers shall differentiate between established accreditation boundary (system boundary, facilities, equipment, etc.) and the external interfaces with other equipment or systems. Established boundaries should include all facility equipment that is to be addressed in the C&A; therefore, the Information System(s) (IS) facilities and equipment must be under the control of the DAA.

Any information-transmission device with a wireless connection to a network (such as WLAN) shall have its air and network interface access ports protected from unauthorized users by FIPS 140-1/2 Overall Type 1 or better encryption. The protection shall extend from the wireless device up to the premise router on the DOD network and shall use DOD PKI based I&A.

The use of radio frequency (RF) wireless computer-direct input technology for computer equipment (such as, keyboard, mouse) is not approved for use in any system with a connection to SIPRNET or other classified computer processing or transmission. Infrared (IR) direct input devices are approved for use on SIPRNET in controlled restricted area environments only. These areas must not have transparent windows or other openings that might allow the projection of the IR signals outside of the restricted area. NIPRNET RF wireless and IR computer-direct input devices are approved within controlled spaces for unclassified computer input.

JTF/Component Commanders will establish wireless usage policy. Usage policy will include as a minimum the following items.

a. Use or prohibition of personal wireless devices not connected to DOD system but operating within controlled areas. This includes peer-to-Peer connections and closed wireless LANs used for gaming and other MWR purposes.

b. Guidelines for use of wireless systems by DOD contractors and other agencies operating in controlled areas. At minimum contractors must register all wireless devices in use at a particular location and follow the guidelines in paragraph 3.c unless prohibited by their contract.

c. Due to the risks presented by wireless devices the following minimum-security precautions will apply to all non DOD wireless implementations.

(1) To facilitate identification of authorized wireless devices, all non DOD wireless devices will be registered with the site TASO. The TASO will provide the wireless Service Set Identification (SSID) (32-character unique identifier) to be used by the devices. Contractors may recommend a wireless SSID to the TASO as long as it is different from the vendors default value. The wireless SSID will not provide any information about the location or user.

(2) Users will sign a user agreement that outlines policy and clearly states all restrictions imposed on the wireless devices, such as not connecting to any DOD network. The agreement will include consent to monitor that states that their wireless connection may be probed as part of vulnerability compliance testing.

(3) All non DOD wireless devices will utilize the strongest level of Wireless Encryption Protocol (WEP) supported by the devices. WEP is not a security solution but it does add an additional obstacle that must be overcome by an adversary. Users will be encouraged to utilize additional FIPS 140-1 or 2 encryption as indicated in 3 b (1) above.

(4) No DOD device may ever be connected to a non DOD wireless network.

(5) Users will notify the TASO when registered wireless devices are no longer required.

(6) DOD personnel using non DOD wireless devices will be directed to use the DOD licensed antivirus and personal firewall software approved for personal use. Non DOD personnel will be encouraged to purchase and use these software products.

Devices that do not require wireless should not be purchased with that capability. All devices procured with wireless capability that is not required will have the capability removed or deactivated. Only authorized person will be able to reactivate the feature.

All Component/JTFs will include wireless scanning as part of their vulnerability testing program.

This page intentionally left blank.

TAB N Certification and Accreditation

1. Purpose

This policy is to identify the requirements and procedures for certifying and accrediting SIPRNET and NIPRNET circuits within the NETWORK.

2. Background

Certification is the process of thorough security testing designed to identify and mitigate systemic vulnerabilities. Accreditation is a specific official authorization and approval. It is granted to operate a network or allow a system to process data of a particular sensitivity level, based on a particular configuration, using a particular mode-of-operation, in a particular environment. This authorization specifies safeguards against defined threats and addresses the vulnerabilities and countermeasures for a given operational environment.

3. Accreditation Responsibility

Designated Approving Authority (DAA) responsibility is intrinsic to the Commander. The Commander may delegate DAA authority within their Command. Such delegation must be in writing, and a file copy of the appointment sent electronically to the cognizant theater COCOM J6. Delegation of DAA authority shall be made to a responsible officer of appropriate technical security experience at a minimum pay grade level of O6/GS-15. Waiver for delegation to a lower grade officer must be obtained from Joint Staff. Responsibility is not delegated from the Commander. The DAA must have the ability to shut down network processes and to channel Command resources toward the mitigation of vulnerabilities through implementation of countermeasures to reduce risk to network/enclave and the Command Mission. Such authority delegation conveys with it the title of Command's or Unit local "DAA". The local DAA shall ensure the accreditation of all collateral and UNCLASSIFIED Automated Information Systems (AIS) that reside on/within the Command or Unit's local networks/enclaves. The DAA is the accrediting authority that accepts security responsibility on behalf of the Commander for the operation of networks and officially declares that a specified system will adequately protect information.

a. DAAs shall ensure that all systems are certified and accredited in accordance with DOD Information Technology Security Certification and Accreditation Process (DITSCAP) procedures found in DOD 8510.01, DOD 5200.40, CJCSM 6211.02B and service regulations. The respective J6, G6, C6, A6, or N6 within Component Commands are responsible to the designated local DAA (whether or not this is the same individual) for validating the risk assessment and accreditation of their respective organizational networks prior to connectivity with any Global Information Grid (GIG) or Standardized Tactical Entry Point (STEP)/Teleport.

b. The DAA of the command element of a deploying Task Force or Joint Task Force will assume the responsibility for risk assessment and accreditation for systems and networks of that organization prior to connectivity with any DISA AIS.

c. AISs operating in a compartmented or multi-level mode or located in a high-risk area are to be given the highest priority for accreditation by local DAAs, because of the risks associated with AIS operation.

d. Local DAAs requiring interconnection of systems with different classification requires individual system accreditation. All cross-domain connections require cognizant theater COCOM and Joint Staff validation, Cross-Domain Technical Advisory Board (CDTAB) review and GIG Security Accreditation Working Group (GIGSAWG) approval. In some instances the interconnection will have to be approved by the GIG 09 Flag Plan, which consists of the Defense Information Agency (DIA), DISA, Joint Staff and National Security Agency (NSA) DAAs.

e. Local DAA accrediting networks will include appropriate documentation such as Memorandum of Agreement (MOA), diagrams and accreditation letters, etc., from all echelons below the GIG STEP/Teleport, Integrated Tactical Strategic Data Network (ITSDN) access point.

SIPRNET Accreditation Requirements. DAAs of commands connecting directly to GIG STEP/Teleport sites for SIPRNET access are required to submit accreditation documents to receive either an Approval to Connect (ATC) or Interim Approval to Connect (IATC) from the DISA SIPRNET Connection Approval Office (SCAO).

a. The local DAA will complete a letter of accreditation: Interim Approval to Operate (IATO) or Approval to Operate (ATO). The accreditation letter will contain the following information: Organization's letterhead; date of signature, Communication Circuit Service Designator (CCSD) (if available); security mode of operations; data classification level; interconnections to other systems; defined level of risk; specified period of time (IATO- up to one year and ATO up to three years); specified operational environment; signature block and signature of DAA.

b. The local DAA will provide network topology drawings. The network diagram will depict the following information: gateways; bridges; routers; switches; High Assurance Guards (HAG); firewalls; encryption devices; interfaces to external and internal LANs and WANs; connections to the DISA node label with the CCSD; Router Port Number (RTRP); and IP addresses. If the SIPRNET is extended to other physical locations, the connections must be depicted in the drawings, as well as the identifier for the location, (such as, building number).

c. The local DAA will provide a Consent to Monitor (CTM) statement with the following information; organizations letterhead; date of signature; Consent to Monitor heading with CCSD; reference the Chairman of Joint Chief of Staff Instruction (CJCSI) 6211.01_ latest version; statement acknowledging that DISA will conduct periodic monitoring of SIPRNET and consent to conducting an initial and unannounced vulnerability assessment; and the signature of the DAA. Note: The CTM and IATO requirement can be address in one letter.

d. The local DAA will complete the DISA SIPRNET Connection Questionnaire (SCQ). The SCQ must have the following information, if available: The CCSD; Router Port Identifier;

organizations name; location; date; Plain Language Address (PLA); site Point of Contacts; network name; premise router IP address; network IP address ranges; "Yes or No" responses to eight questions. All "YES" responses on the questionnaire must be explained.

(1) Identify uncleared contractors, non-DOD, or foreign nationals, with physical access to areas where workstations are directly or indirectly connected to the SIPRNET.

(2) Identify foreign national that have network access to the SIPRNET.

(3) Identify US network or coalition network that may be tunneled over the SIPRNET backbone (such as, CENTRIXS).

(4) Identify interconnections of systems of different classification with a Cross-Domain Solution (CDS) (that is, network switching devices or high assurance guards) and ensure the CDS ticket number is annotated in question number ten of the SCQ.

e. The JTF or Component J6 Operations section will submit a Gateway Access Request (GAR) that includes the planned ITSDN termination technical data. Prior to, or concurrent with submission of the GAR, the JTF or Component DAA will submit the SIPRNET Accreditation Requirements packages. Regional DISA Contingency/Exercise Branch Office, with the concurrence of the cognizant theater COCOM J6, will issue will issue Gateway Access Authorization (GAA) messages with the technical data required to terminate approved STEP/Teleport ITSDN connections. The Regional DISA Contingency/Exercise Branch Office will not issue the GAA without the verifying that an accreditation package is on file or being processed by the DISA SIPRNET Connection Approval Office (SCAO).

f Connections made directly to Global Information Grid (GIG) ITSDN gateway routers from the NETWORK are defined as Tier 1 connections. It is the responsibility of the deployed JTF DAA or in the case of an independent force, the Component/Tier 1 DAA, to ensure network security at the Tier 1 operating level and below. The JTF or Component DAA shall submit accreditation documentation to the cognizant theater COCOM J6 for validation. The COCOM J6 will track and forward documents to the SCAO. The SCAO shall validate each request and approve/disapprove NETWORKSIPRNET accesses accordingly. The SCAO will identify discrepancies as soon as possible and return the packages for correction/clarification. Returned accreditation packages must be resubmitted in a timely fashion. Failure to correct or update information identified by the SCAO may result in a package being rejected without granting an Interim Approval to Connect/Approval to Connect. In some cases the SCAO may identify security areas that require change. The JTF/Component DAA is responsible for mitigating the identified security findings and re-submitting the accreditation package.

g. The JTF or Component/Tier 1 DAAs must include subordinate network accreditation documentation in the overall SIPRNET accreditation package submitted to the cognizant theater COCOM J6 for validation Operating echelons below Tier 1 are responsible to the JTF or Component/Tier 1 DAA for providing the appropriate accreditation documentation. That documentation shall include the following documents: Memorandum of Understanding/Agreement (MOU/MOA); letter of accreditation; network drawings. The

network diagrams will include the following information: Gateways; Bridges; Routers; Switches; High Assurance Guards (HAG); Firewalls; encryption devices; Interfaces to external and internal LANs and WANs; Connections to the DISA node label with the CCSD; Router Port Number (RTRP); IP addresses. If SIPRNET is extended to physical locations outside the enclave boundary, network drawings shall depict each connection, complete with Communication Circuit Service Designator (CCSD), physical location, country, site, camp, unit, and building number.

4. NIPRNET Accreditation Requirements

DAAs of commands connecting directly to GIG STEP/Teleport sites for NIPRNET access are required to accredit the connectivity between their local enclave and the GIG.

a. The JTF or Component/Tier 1 DAAs will submit accreditation documents, which include a letter of accreditation, Consent to Monitor (CTM), and network diagrams. All documents are signed by the JTF or Component/Tier 1 DAA, scanned, and emailed to the cognizant theater COCOM J6. The NIPRNET Connection Approval Process (NCAP) office will issue an IATC/ATC after receiving and approving the CAP package.

b. The JTF or Component/Tier 1 DAAs must include subordinate network accreditation documentation in the overall NIPRNET accreditation package submitted to the cognizant theater COCOM J6 for validation Operating echelons below Tier 1 are responsible to the JTF or Component/Tier 1 DAA for providing the appropriate accreditation documentation. That documentation shall include the following documents: Memorandum of Understanding/Agreement (MOU/MOA); letter of accreditation; network drawings, to include the following annotations: Gateways; Bridges; Routers; Switches; High Assurance Guards (HAG); Firewalls; encryption devices; interfaces to external and internal LANs and WANs; connections to the Tier 1 node labeled with the CCSD; Router Port Number (RTRP); and IP addresses. If NIPRNET is extended to physical locations outside the enclave boundary, network drawings shall depict each connection, complete with Communication Circuit Service Designator (CCSD), physical location, country, site, camp, unit, and building number.

c. The GIG connection approval procedures may be obtained at the DISA SIPRNET Information Assurance Support Environment (IASE) at http://cassie.iiie.disa.smil.mil

5. Post Interim Accreditation

a. The JTF or Component/Tier 1 DAAs will maintain documentation describing various operational and security aspects of the system via a System Security Authorization Agreement (SSAA). All site DAAs connecting to the GIG are required to complete a SSAA in order to accredit and receive an ATC from the SCAO. The SSAA is the Defense Information Technology Security and Accreditation Process (DITSCAP) DOD 5200.40, requirement to fully accredit an AIS or network.

b. JTF or Component/Tier 1 DAAs will coordinate with cognizant theater COCOM J6s to schedule SIPRNET Compliance Validation (SCV) inspections. At a minimum, SCVs are completed annually.

TAB O System Vulnerability Assessments

1. Purpose

The purpose of this Tab is to define responsibilities and requirements associated with system vulnerability assessments prescibed for systems connected to the NETWORK .

2. Overview

Phase IV - Post Accreditation, is outlined in the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) (DOD Instruction 5200.40). The Post Accreditation phase includes activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, periodic compliance validation reviews and periodic vulnerability assessments are conducted as part of this phase. Vulnerability assessments consist of external and internal vulnerability scanning and the use of an automated tool sets, or manual review, to discover incorrectly configured systems. Security configuration baselines are based on applicable NSA configuration guides, associated DISA addendums, DISA Security Technical Implementation Guides (STIG); and vendor security configuration guides that have been endorsed by NSA and/or DISA.

3. Policy

The Terminal Area Security Officer (TASO) at each deployed site accessing NETWORK services is responsible for performing periodic vulnerability assessments on every network device. Assessments will be conducted as directed in the System Security Authorization Agreement (SSAA), within 60 days of the establishment of a new network or change of controlling unit (COR). The assessment will consist of vulnerability scans, a Security Readiness Review of a sample of systems, resolution of identified vulnerabilities, and attendant documentation.

DISA Vulnerability Management System (VMS) Security Readiness Review Database (SRRDB). DISA Field Security Operations (FSO) maintains the SRRDB. The SRRDB may be used to automate documentation and track site vulnerabilities identified during periodic assessments or formal visits. The SRRDB has an automated capability to populate the database with Internet Scanner and SRR script results. Cognizant theater COCOM J6s will access to all theater related vulnerability data; identified JTF and Component IA personnel may have access to related and specific site vulnerability data, and identified site IA personnel may have access to their network's vulnerability data. Personnel must complete the DISA Form 41 to gain access to VMS; contact cognizant COCOM J6 for required documentation and detailed instructions.

Security Readiness Review (SRR) Scripts. DISA FSO maintains SRR scripts to evaluate a system's configuration compared to the requirements in the applicable STIG. The scripts are run from the system being evaluated and the results file is used to populate the SRRDB. Scripts can be downloaded from http://cassie.iiie.disa.smil.mil/techguid/SRR/index.html.

Internet Security Systems (ISS) Internet Scanner. Internet Scanner is the recommended software with which to carry out vulnerability scanning. DISA will make the software available to specific site personnel that have either successfully completed the DISA FSO sponsored Internet Scanner training or have successfully passed the final examination. If using Internet Scanner, load the DISA "Full" policy, available at http://cassie.iiie.disa.smil.mil/techguid/ iss/index.html. Other software that performs system vulnerability assessments can be used as long as all other requirements in this Tab are met.

Vulnerability Scanning. Vulnerability scanning refers to the automated or manual process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. Vulnerability scanning typically employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an organization can use to tighten the network's security. Vulnerability scans will be conducted with the latest release and update of Internet Scanner or other software provided by the applicable Service. Personnel performing the scan must be very familiar with the software to eliminate the potential of adverse network impact. Follow Internet Scanner or Service specific notification procedures prior to conducting the scan. Ensure the cognizant theater COCOM J6, DOD-CERT, DISA RCERT, Service CERT, and Service Local Control Centers are informed prior to any scanning. Scanning may inadvertently cause intrusion alerts on network security devices.

a. External Vulnerability Scanning. External scans are conducted from a location beyond the sites security perimeter, such as outside the perimeter/border/gateway router. External vulnerability scanning focuses on; identifying open ports and services on inbound permanent connections, on discovering information about internal network assets, and on providing a remote access policy review. External vulnerability assessments are required if the perimeter security devices are configured to allow the source IP of the scanning device unimpeded access to network devices.

b. Internal Vulnerability Scanning. Internal scans are conducted from a location within a particular enclave, such as,inside the innermost router. Internal vulnerability scanning focuses on; assessing the threat of rogue software or malicious employees in an enterprise, providing server vulnerability assessments, firewall policy review, Virtual Private Network (VPN) policy review, and router and switch open port and services scan.

c. Formal Vulnerability Assessment Visits. Cognizant theater COCOMs', with the support of NSA and DISA, may perform vulnerability assessments of Network installations. These assessments will consist of an internal vulnerability scan and Security Readiness Reviews of a sample of onsite systems. Internet Scanner, using the DISA "Full" policy (available at http://cassie.iiie.disa.smil.mil/techguid/iss/index.html) may be used during the formal visits. The results will be used to populate the SRRDB. The inspection team will out brief the local TASO and DAA, and the 'visit' results will be made available to the cognizant theater COCOM J6.

Wireless. All networks will periodically be scanned for the presence of wireless networks and/or connections operating on the site. Unauthorized wireless systems will be deactivated when they are detected.

Vulnerability Resolution. Vulnerability resolution begins immediately and my run concurrent with further assessments. Actions taken must be tracked and codified in either the SRRDB or in local documentation.

Documenting Assessments. The preferred method of tracking vulnerabilities is the SRRDB. Tools are available to populate the SRRDB with Internet Scanner and SRR script results. If the assessment results cannot be entered into the SRRDB, the site will maintain documentation locally and provide an electronic copy to the cognizant theater COCOM J6 via email. The documentation will reference the dates of assessments, identify who performed the assessment, name the systems assessed, provide results of the assessment, and provide the status of identified vulnerabilities. A site that maintains the documents locally will have the last two (2) assessments available for cognizant theater COCOM J6 review.

Vulnerability Assessment Assistance. Components should request assistance with vulnerability assessments through Service IA channels. Cognizant theater COCOM J6 may assist JTF and Components with requests for NSA, DISA FSO or other Service support if required.

This page intentionally left blank.

TAB P IA Architecture

1. Purpose

The purpose of this tab is to present an Information Assurance (IA) physical and logical architecture that both reflects the Joint Users Interoperability Communicatoins Event 2006 Exercise Directive (JUICE 06) IA policy and procedures discussed throughout this appendix; and is representative of IA capabilities currently available to Joint Force headquarters, Components and subordinate units.

2. General

a. Interoperability and integration of IA solutions within or supporting the NETWORK will be achieved through adherence to an architecture that will enable implementing a defense-in-depth approach.

b. Layers of technical and non-technical solutions will be employed to:

(1) Provide appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation to information and resources to NETWORK users.

(2) Defend deployed enclave perimeters.

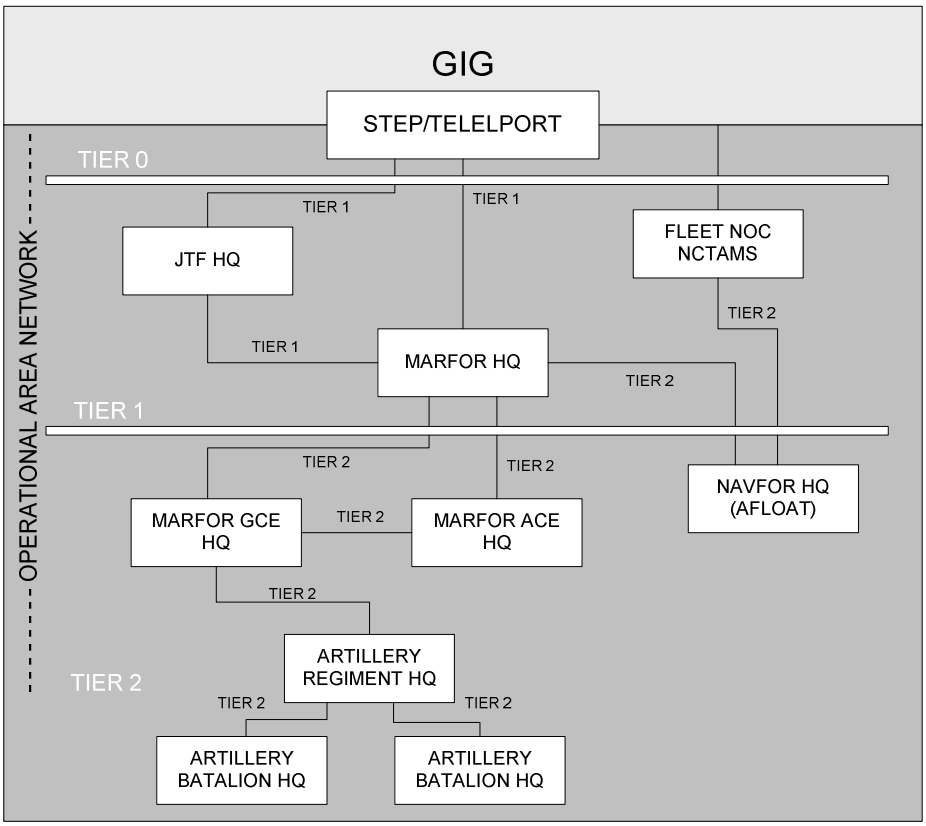
(3) Protect information systems, enclaves and computing environments (including applications and databases) from external and internal threats.

(4) Use supporting infrastructures such as common access card (CAC), public key infrastructure (PKI), biometrics, modernized cryptographic capability and key management infrastructure (KMI) to enforce IA requirements.

(5) Implement a protected IA architecture for incident identification and response capabilities.

c. The NETWORKIA architecture is driven by an enterprise-wide look at the entire supported theater area of responsibility (AOR). The GIG Standardized Tactical Entry Points (STEP)/Teleports are identified as Tier O of what will be described as a three tier network connection hierarchy. Direct connections into a STEP/Teleport are made from the first deployed level or Tier 1. JTF headquarters, JSOTF headquarters and JTF Component headquarters normally operate as Tier 1 nodes. The connection between Tier 0 and Tier 1 are labeled as Tier 1 connections. Connections between two Tier 1 locations, such as JTF headquarters to MARFOR headquarters, are also labeled as Tier 1 connections. Sites that are provided data services solely through connections to a Tier 1 node are labeled as tier 2. An example of this type of Tier 2 connections may be that of a MARFOR headquarters connected to its subordinate Ground Combat Element (GCE) headquarters. The connection is also labeled as Tier 2. Sites that receive data services through connection to a Tier 2 node are also labeled as Tier 2 and so is the connection. An example here would be that of a

Marine GCE headquarters connection to its subordinate Artillery Regimental Headquarters. The diagram below provides a depiction of IA Tiers within the NETWORK. The headquarters nodes are a representative sample of potential deployed forces.



3. Connection Requirements

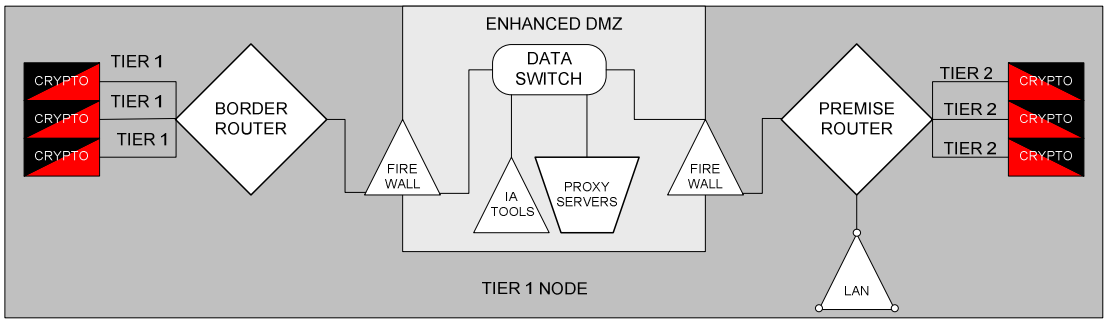
a. Tier 1. Tier 1 connections are made between the STEP/Teleport Integrated Tactical Strategic Data Network (ITSDN) direct connect routers and Tier 1 lever Border routers (Border routers are also known as 1/1 routers, Perimeter routers, Screening routers or Gateway routers.) or between two Tier 1 level Border routers. Tier 1 connections use Border Gateway Protocol 4 (BGP-4) as a routing protocol. The transmission paths carrying the data circuits require Transmission Security (TRANSEC) encryption devices (unless the path is via fiber optic cable). SIPRNET circuits require additional circuit level encryption.

b. Tier 2. Tier 2 connections are made between Tier 1 level Premise routers (Premise routers at Tier 1 are also known as 1/2 routers or Interior routers.) and Tier 2 level Premise routers or between two Premise routers. Tier 2 connections normally employ an internal routing protocol such as Enhanced Internal Gateway Routing Protocol (EIGRP) or Open Shortest Path First (OSPF). The transmission paths carrying the data circuits between nodes require Transmission Security (TRANSEC) encryption devices (unless the path is via fiber optic cable). SIPRNET circuits require additional circuit level encryption.

4. Nodal Requirements

a. Tier 1

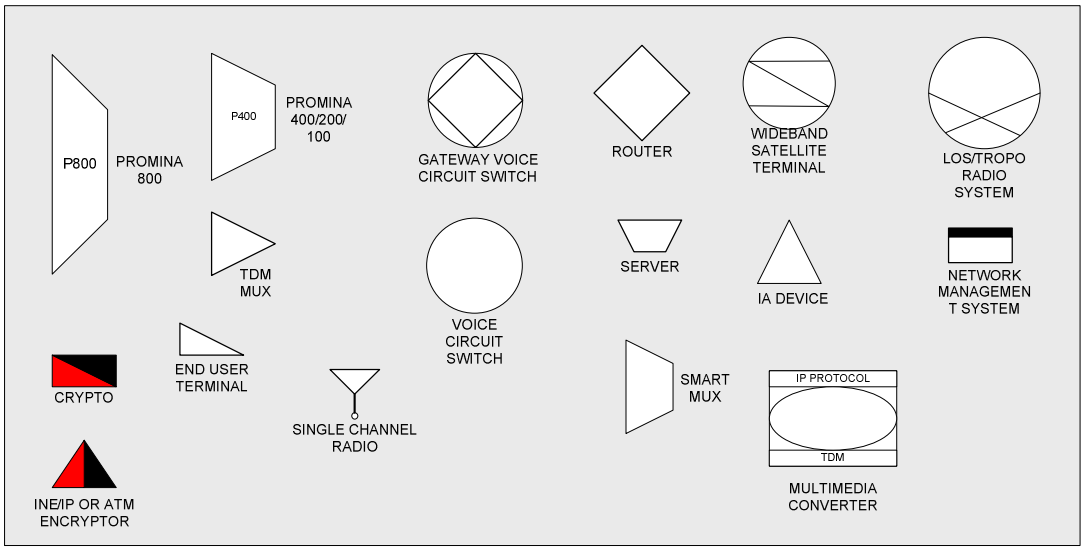
(1) The diagram below depict a generic deployed Tier 1 data gateway node.



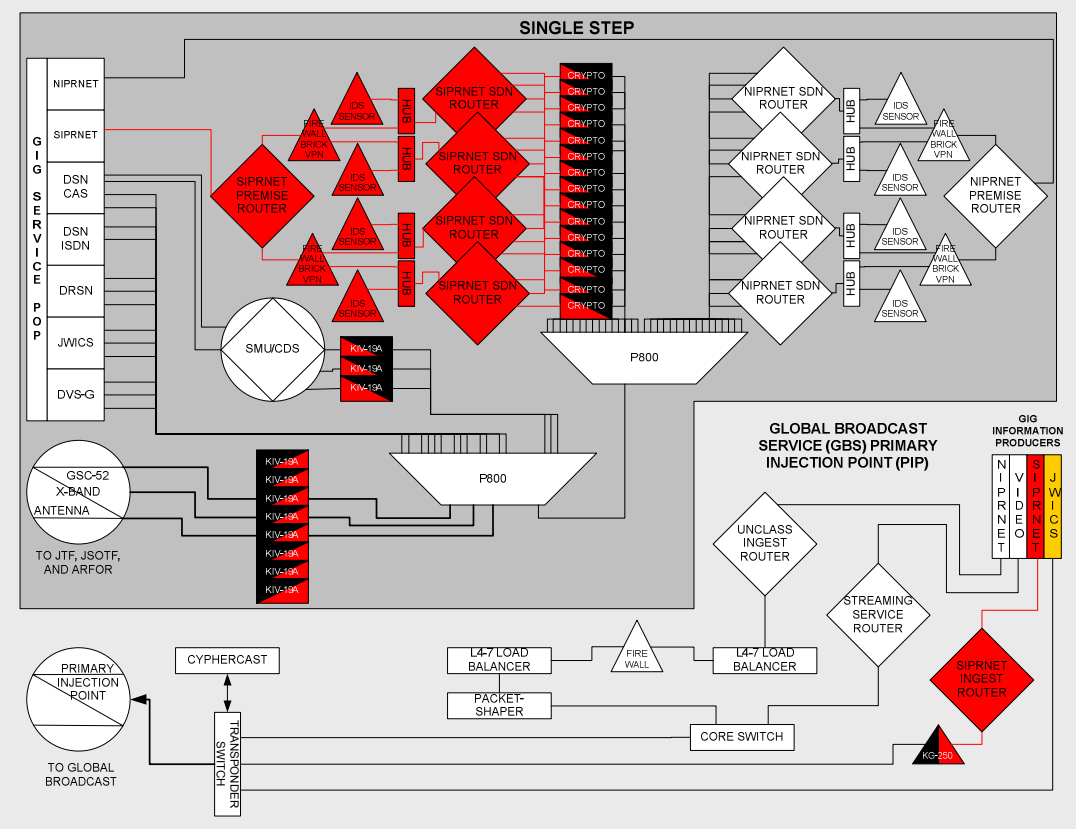
(2) The Tier 1 node provides the baseline perimeter protection to its own networks and those subordinate Tier 2 nodes receiving access to NETWORK services behind it. It is characterized by a Tier 1 Border router (1/1), a standard or enhanced Demilitarized Zone (DMZ), an IA tool suite and a Premise router (1/2) servicing protected local network users and subordinate unit nodes.

b. Tier 2. The Tier 2 node resides behind a Tier 1 node. At a minimum Tier 2 nodes must have firewall protection.

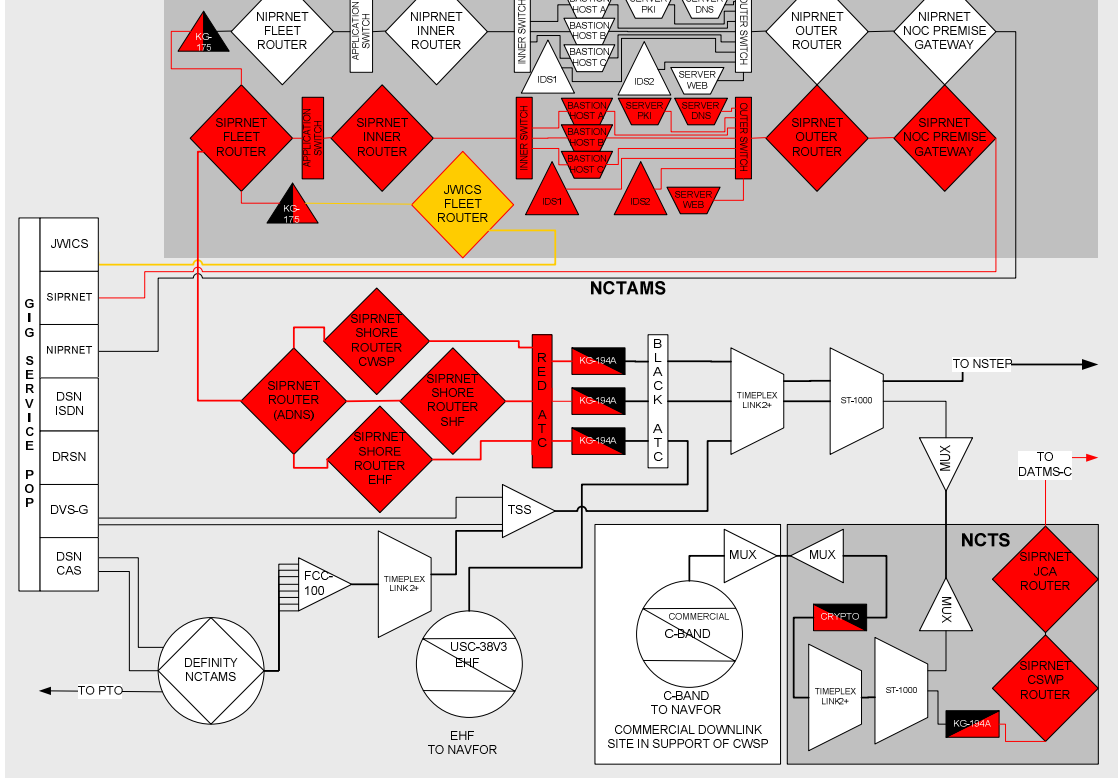
c. Example Network configurations. The shapes identified below provide legend information to the diagrams that follow.



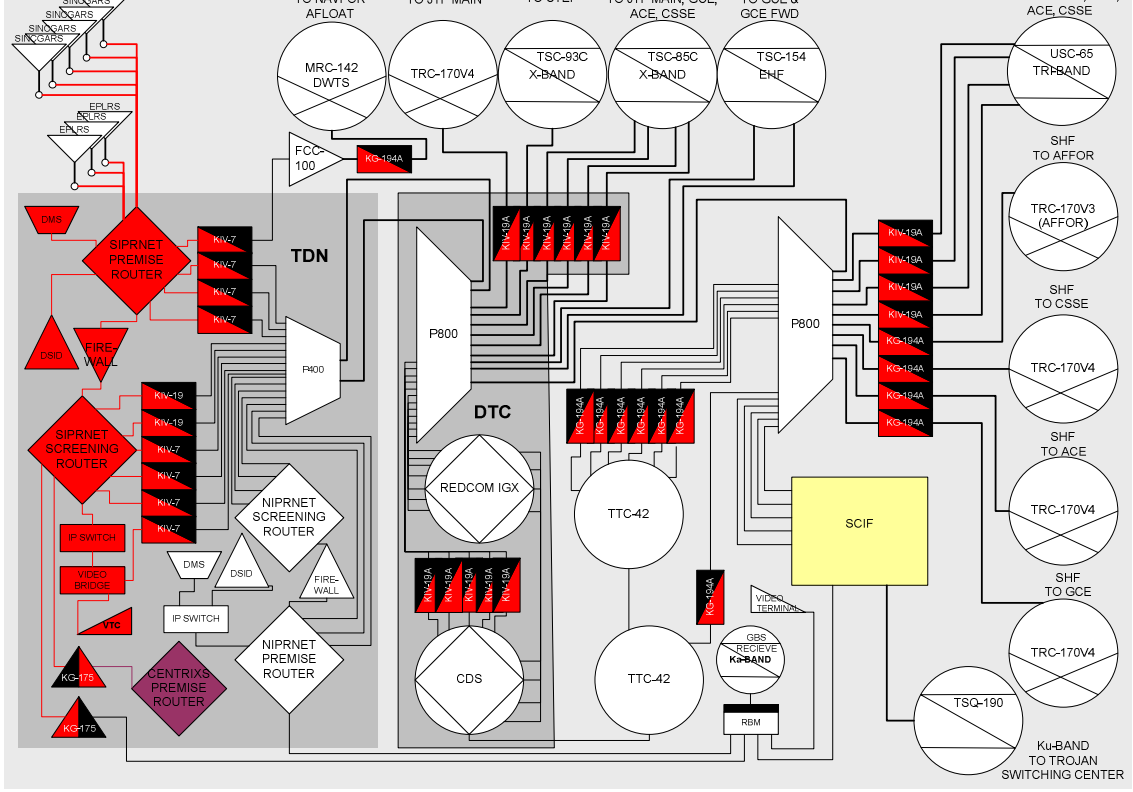
from the PIP are treated as Tier 2 type connections.



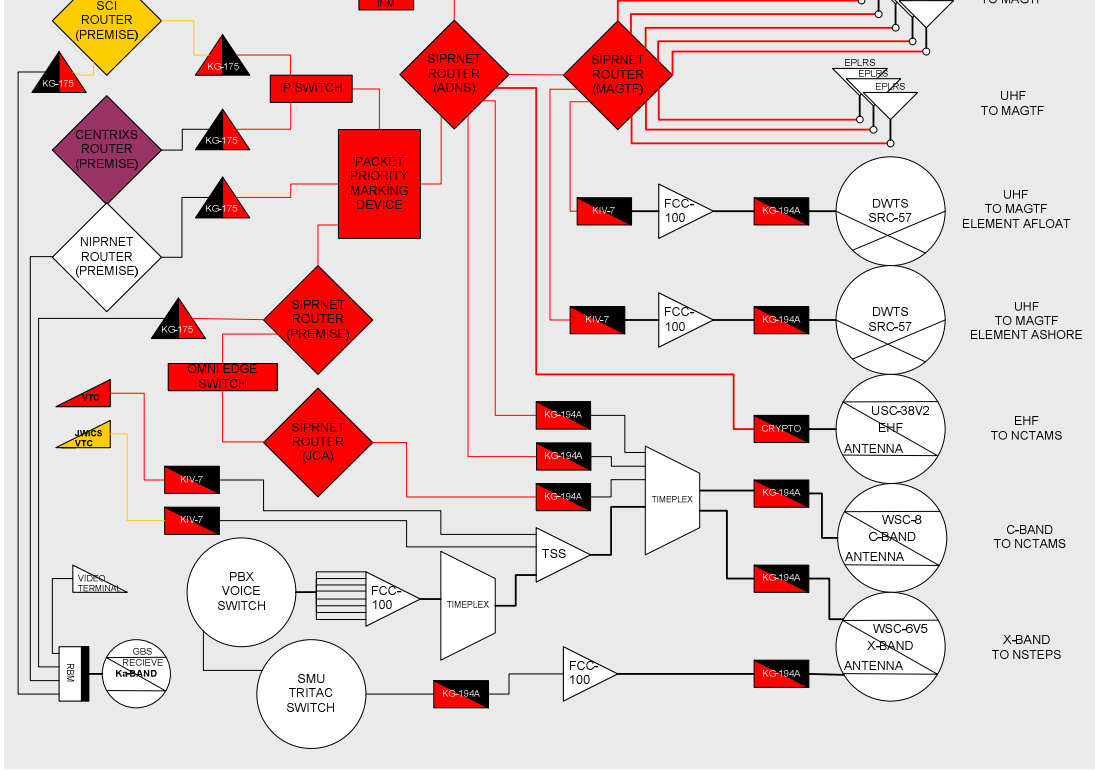
(2) Representative Fleet NOC/NCTAMS. Note connections into the GIG. Services are extended to deployed Navy users via Tier 2 type connections.



(3) Representative JTF Component. Note Tier 1 type connections from screening (border) routers to STEP, JTF and other JTF Components less the NAVFOR. Tier 2 type connections are made from the premise router to the NAVFOR and MARFOR subordinates.



(4) Representative NAVFOR (Afloat) using Tier 2 type connections into the NCTAMS Tier 1 and the MARFOR.


SCI ROUTER (PREMISE)
KG-175
KG-175
IP SWITCH
SIPRNET ROUTER (ADNS)
SIPRNET ROUTER (MAGTF)
EPLRS
EPLRS
EPLRS
UHF TO MAGTF
CENTRIXS ROUTER (PREMISE)
KG-175
PACKET PRIORITY MARKING DEVICE
KG-175
NIPRNET ROUTER (PREMISE)
KIV-7
FCC-100
KG-194A
DWTS SRC-57
UHF TO MAGTF ELEMENT AFLOAT
KIV-7
FCC-100
KG-194A
DWTS SRC-57
UHF TO MAGTF ELEMENT ASHORE
KG-175
SIPRNET ROUTER (PREMISE)
OMNI EDGE SWITCH
VTC
JWICS VTC
SIPRNET ROUTER (JCA)
KG-194A
KG-194A
KG-194A
CRYPTO
USC-38V2 EHF ANTENNA
EHF TO NCTAMS
KIV-7
KIV-7
TIMEPLEX
KG-194A
WSC-8 C-BAND ANTENNA
C-BAND TO NCTAMS
TSS
KG-194A
VIDEO TERMINAL
PBX VOICE SWITCH
FCC-100
TIMEPLEX
WSC-6V5 X-BAND ANTENNA
X-BAND TO NSTEPS
RBM
GBS RECIEVE Ka-BAND
SMU TRITAC SWITCH
KG-194A
FCC-100
KG-194A

This page intentionally left blank.

TAB Q Quality of Service (QoS) Policy

1. Purpose

This tab will outline a deployment scenario for all nodes across the network. The basic QoS policy described herein falls within the cognizant of the Theater Combatant Commanders through their J6 offices.

2. General

a. Definition. Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the building blocks that will be used for future business applications in WAN, and service provider networks.

b. Network Convergence. Network convergence is the joining of voice, video, data and legacy services on a single Internet Protocol (IP) network. Convergence results in considerable cost savings and creates network efficiencies that cannot be obtained on networks built in a stovepipe fashion.

1) Management of network resources in a converged network is a necessity. Successful convergence of voice, video and data can only be achieved through a well-planned deployment of QoS. The following are some benefits of QoS:

a) Provides network managers with deterministic control over network resources and allows management of the network from a business, rather than a technical, perspective.

b) Ensures time-sensitive and mission-critical applications have the resources they require, while allowing other applications controlled access to the network.

c) Improves user experience.

d) Reduces costs by using existing resources more efficiently, thereby delaying or reducing the need for expansion and/or upgrades. It is not an indefinite substitute for bandwidth, but ensures existing bandwidth resources are used in an efficient manner.

2) QoS ensures all applications receive an equitable share of network resources based on assigned priority and network characteristics. Voice quality is dependent on a low latency, low jitter and a low packet loss connection. It is imperative that voice services be aligned with the strict priority queue and low latency queuing (LLQ). Other applications may operate most effectively in an environment sans one or a combination of typical transmission quality factors, aligning most appropriately with

either a mission critical or best effort queue. Creating a network environment that caters to the unique characteristics of each application or each type of application is required in a converged network.

3. Policy

NETWORK QoS policy will consist of four classes of service – Voice, Mission Critical Data, Best Effort Data and Scavenger Data. Details of each of the four classes of service follow:

a. Voice Class. The Voice Class will ensure voice bearer traffic is guaranteed a percentage of the bandwidth. In addition, since Voice over Internet Protocol (VoIP) is sensitive to variations in transmission quality, its packets will receive preferential treatment over all other network traffic. In this Low Latency Queuing (LLQ) implementation, this strict priority queue will completely empty before any other queues are serviced.

NOTE: The voice queue bandwidth allocation must match the Call Admission Control settings in the VoSIP/VoIP Call Manager (regions/locations). If the IP telephony system is allowed to accept calls beyond its bandwidth allocation in the QoS implementation, users will experience less than desirable call quality and/or call failure. In most cases, bandwidth should be calculated using the G.729 codec rates with all overhead included in the calculation (37kbps @ 50pps/802.1q). Additionally, it is imperative for remotely-supported voice instruments to be accurately organized by location in order to ensure compliance with remote WAN bandwidth allocation. If/when G.711 codec rates are required, network administrators should accurately account for the bandwidth requirements using the call manager CAC feature (G.711 over 802.1q is 93kbps @ 50pps).

b. Mission Critical Class. The Mission Critical Class will provide assured forwarding for services deemed mission critical. In most cases, data allowed into the Mission Critical Queue should be limited to that which is interactive in nature. NETWORK policy will ensure network control traffic (routing (BGP), Active Directory (AD) and call signaling), and near-real time data feeds are included in this class. It is very important to minimize the number of applications given mission critical status to ensure the class is not diluted into a state that is equal to the best effort class.

c. Best Effort Class. The Best Effort Class provides service to all applications that are less sensitive to variations in transmission quality and/or are considered useful but not mission critical. Email, for instance, comes with its own queuing mechanisms. If the network is congested, email will simply queue up within the email server until there is sufficient bandwidth for delivery. Web and data replication traffic will traverse the network slower in periods of congestion. Their delivery is not dependent on error free, real-time availability of network resources.

d. Scavenger Class. The Scavenger Class is the most effective tool for managing the deferential treatment of traffic. This class can be used to minimize the effect of worms and other network attacks. It can also be used to limit the use of official network resources

during periods of congestion. When the network is not congested, traffic aligned with the Scavenger Class will flow at the maximum availability of bandwidth.

4. Deployment

a. Implementation. The Cisco Modular QoS Command Line Interface (MQC) provides a straightforward means of implementing a well-defined QoS policy. In its most simplistic form, the QoS policy can be implemented by Classifying and Marking on ingress interfaces and Queuing on egress interfaces. These processes, along with the inclusion of bandwidth constraints on each class of service are forms of Congestion Management. There are also Congestion Avoidance tools within the QoS arsenal. For instance, the Mission Critical class will actually consist of multiple classes of traffic (see Table 1). Class-Based Weighted Random Early Detection (CBWRED) will be used to prioritize the handling of traffic within that queue.

b. Tier-1 / Distribution Classification. At the Tier-1 (Tier-1/2), traffic will be classified and marked according to the Traffic Classification Template. This will create a trust boundary between tactical and Tier-2/Tier-3 networks and the distribution and core architectures. This boundary is required in order to allow network end-points to classify and mark traffic according to Intra-theater priorities. Likewise, the boundary will ensure all enterprise-wide information flows happen in a manner that is in compliance with the Theater COCOM/NETWORK policy.

c. Tier-1 Traffic Classification Template

Traffic	DSCP	PHB	COS	Description
Voice (Bearer)	46	EF	5	Voice bearer traffic
DCTS/I-Video	34	AF41	4	DCTS (Interactive video & associated voice)
GCCS	26	AF31	3	COP Sync Tools
C2PC	26	AF31	3	C2PC
Custom1	18	AF21	2	Transactional Data (Database Access, etc)
Custom2	10	AF11	2	Bulk Data (Synchronization, File Transfers/Mirror, etc)
IP Routing	48	CS6	6	BGP
Voice (Signaling)	24	CS3	3	Voice call-signaling
Active Directory	16	CS2	2	Kerberos, LDAP, etc
Network Mgmt	16	CS2	2	SNMP, Syslog, DNS, etc
Best Effort	0	0	0	All other applications (Web, SMTP, etc)
Scavenger	8	CS1	1	Known worms, forbidden web sites, etc

d. Tier-2 / Access Classification

1) Industry literature suggests that QoS is required wherever there is a potential for congestion. While not as distinct as the congestion one might experience at the Wide Area Network (WAN) edge, the Local Area Network (LAN) can experience

congestion between the access and distribution infrastructures and between the distribution and core infrastructures. This congestion is evident wherever a bandwidth allocation is made in a statistical fashion and is typical for access to distribution, server to distribution and distribution to core connections.

2) Congestion will also be experienced on any Intra-theater or Tier-2 WAN links, which is not a component dictated by the Theater COCOM/NETWORKEnterprise QoS Policy. All LAN and Tier-2/Tier-3 QoS implementations are the responsibility of Component and Joint Task Force (JTF) elements. NETWORK policy recommends adoption of the same QoS policy for both infrastructure areas, but allows for flexibility should site-specific mission requirements dictate a unique prioritization of traffic. For instance, the NETWORK policy recommends setting the Voice Queue to a maximum bandwidth allotment of 33% and the Mission-Critical Queue to a maximum bandwidth allotment of 41%, each becoming effective during periods of congestion (see QoS Bandwidth Allocation table). These allocations can be adjusted by the site for all Tier-2 and Tier-2 WAN connections. Unlike the production queues (Voice, Mission-Critical and Best Effort), the Scavenger class bandwidth allocation should not be allocated more than 1%. This queue is meant to provide deferential treatment to traffic considered a nuisance (peer to peer), a security risk (worms) or of lesser importance than legitimate official traffic (aol, yahoo, etc). Like the other queues, the Scavenger queue will 'rate limit' its traffic during periods of congestion. In reality, this means traffic assigned to the Scavenger Queue will not compete for bandwidth during peak or official hours, but will have bandwidth available during after-hours periods.

3) QoS Bandwidth Allocation

Queue	Service	Bandwidth Allotment
Low Latency Queue	Voice (Bearer)	*33%*
Locally-Defined Mission-Critical Data	DCTS – Interactive Video GCCS/C2PC Net Control (Call-Signaling, IP Routing, AD Protocols) *Custom1* *Custom2*	*41%*
Best Effort	Web Email FTP Remaining legitimate traffic	*25%*
Scavenger	Worm Filtering Streaming Radio/Video Sites Undesirable traffic	1%

4) The traffic classification template (Tier-1 Traffic Classification Template) leaves room for two site-defined mission critical applications. Use of these categories is not

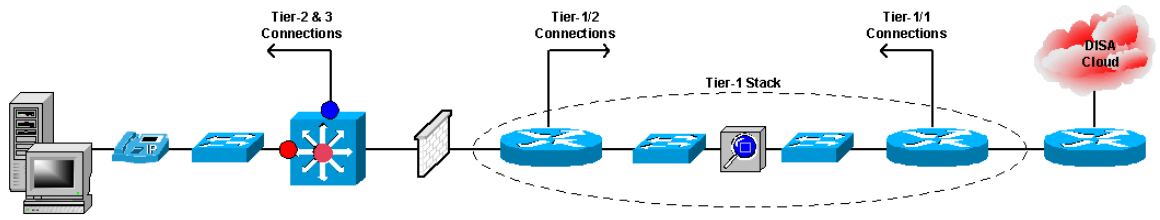
mandated, but we do recommend limiting additions to the Mission-Critical Queue to ensure this queue's effectiveness. Diluting the queue beyond those applications included in the template may yield a traffic class that exhibits performance characteristics equal to the Best Effort Queue – clearly not the intent of the Mission Critical Queue. Like bandwidth allotment, actual classification and marking of the traffic at the Tier-2 may vary from the USCENTCOM policy, depending on site or region-specific priorities.

Implementation. JTF and Components planning to employ converged service strategies must coordinate with the cognizant Theater COCOM J6. The Theater COCOM J6 will coordinate with DISA elements in order to implement the Theater COCOM/NETWORKQoS policy on the DISA Tier-0 or STEP router supporting the entity's connection. The DISA changes will be canned, based on HQ policy, thus it is imperative for the Tier-1 configurations to match the configurations in this document. Likewise, it is imperative that each site submit their Mission-Critical application classification matrix to the Theater COCOM J6 to ensure the DISA configurations take theater priority traffic requirements into consideration.

Exhibits

1-TIER-2 CONFIGURATION EXAMPLE
2-TIER-1/2 CONFIGURATION EXAMPLE
3-TIER-1/1 CONFIGURATION EXAMPLE
4-TIER-0 CONFIGURATION EXAMPLE

EXHIBIT 1 Tier-2 Configuration Example



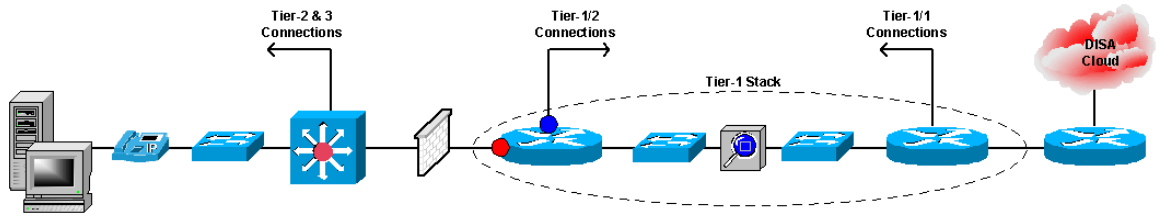
Tier-2: Mark & Classify	Tier-2: Queue

class-map match-all VOICE
  match access-group name VOICE
class-map match-all DCTS
  match access-group name DCTS
class-map match-all GCCS
  match access-group name GCCS
class-map match-all C2PC
  match access-group name C2PC
class-map match-all CUSTOM1
  match access-group name CUSTOM1
class-map match-all CUSTOM2
  match access-group name CUSTOM2
class-map match-all BGP-ROUTING
  match access-group name BGP-ROUTING
class-map match-all VOICE-SIGNALING
  match access-group name VOICE-SIGNALING
class-map match-all ACTIVE-DIRECTORY
  match access-group name ACTIVE-DIRECTORY
class-map match-all NET-MGMT
  match access-group name NET-MGMT
class-map match-any SCAVENGER
 match protocol napster
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 	
policy-map TIER-2-LAN-EDGE-IN
  class VOICE
  set ip dscp ef
  class DCTS
  set ip dscp af41
  class GCCS
  set ip dscp af31
  class C2PC
  set ip dscp af31
  class CUSTOM1
  set ip dscp af21
	class-map match-all
	MARKED_VOICE
	  match ip dscp ef
	class-map match-any MISSION-
	CRITICAL
	  match ip dscp af41
	  match ip dscp af31
	  match ip dscp af21
	  match ip dscp af11
	  match ip dscp cs6
	  match ip dscp cs3
	  match ip dscp cs2
	class-map match-any SCAVENGER
	  match ip dscp cs1
	class-map match-any DEFAULT
	 match ip dscp cs0
	
	policy-map TIER-2-WAN-OUT
	  class MARKED_VOICE
	  priority percent 33
	  class MISSION-CRITICAL
	  bandwidth percent 41
	  random-detect dscp-based
	  class SCAVENGER
	  bandwidth percent 1
	  class DEFAULT
	  bandwidth percent 25
	  random-detect
	
	Interface <TACTICAL WAN>
	  bandwidth <bandwidth>
	  service-policy output TIER-2-
	WAN-OUT

```
  class CUSTOM2
    set ip dscp af11
  class BGP-ROUTING
    set ip dscp cs6
  class VOICE-SIGNALING
    set ip dscp cs3
  class ACTIVE-DIRECTORY
    set ip dscp cs2
  class NET-MGMT
    set ip dscp cs2
  class SCAVENGER
    set ip dscp cs1
  class DEFAULT
    set ip dscp cs0

ip access-list extended VOICE
  permit udp <VoSIP/VoIP IP> any range 16384 32767
ip access-list extended DCTS
 permit  tcp <DCTS Svr IP> eq 80 any
 permit tcp <DCTS Svr IP> eq 8080 any
 permit tcp <DCTS Svr IP> eq 1503 any
 permit tcp <DCTS Svr IP> eq 1720 any
 permit tcp <DCTS Svr IP> eq 7640 any
 permit tcp <DCTS Svr IP> eq 7648 any
 permit udp <DCTS Svr IP> eq 7648 any
 permit udp <DCTS Svr IP> eq 24032 any
 permit udp <DCTS Svr IP> eq 56800 any

*Above is for server to server connections.  If client to
server details are required, please contact J6-CNE.

ip access-list extended GCCS
 permit tcp any any eq 9119
 permit tcp any any eq 9981
 permit tcp any eq 9119 any
 permit tcp any eq 9981 any
ip access-list extended C2PC
 permit udp any any eq 2000
 permit udp any any eq 2701
 permit udp any any eq 2702
ip access-list extended CUSTOM1
 permit TCP any any eq xxxx
ip access-list extended CUSTOM2
 permit TCP any any eq xxxx
ip access-list extended BGP-ROUTING
 permit TCP any any eq 179
ip access-list extended VOICE-SIGNALING
 permit tcp any any range 2000 2002
 permit tcp any any eq 1720
 permit tcp any any range 11000 11999
 permit udp any any eq 2427
```

ip access-list extended ACTIVE-DIRECTORY permit udp any any eq 88 permit udp any any eq 389 permit udp any any eq domain permit tcp any any eq 3268 ip access-list extended NET-MGMT permit udp any eq 161 any permit udp any eq 9995 any permit udp any eq 9996 any Interface <LAN EDGE> Service-policy input TIER-2-LAN-EDGE-IN	

EXHIBIT 2 **Tier-1/2 Configuration Example**



Tier-1/2: Mark & Classify	**Tier-1/2: Queue**

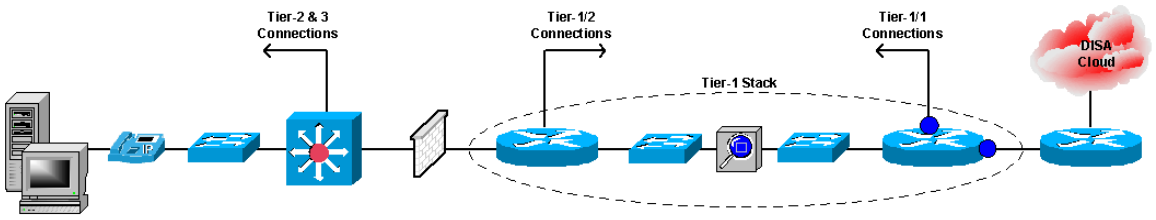
class-map match-all VOICE
  match access-group name VOICE
class-map match-all DCTS
  match access-group name DCTS
class-map match-all GCCS
  match access-group name GCCS
class-map match-all C2PC
  match access-group name C2PC
class-map match-all CUSTOM1
  match access-group name CUSTOM1
class-map match-all CUSTOM2
  match access-group name CUSTOM2
class-map match-all BGP-ROUTING
  match access-group name BGP-ROUTING
class-map match-all VOICE-SIGNALING
  match access-group name VOICE-SIGNALING
class-map match-all ACTIVE-DIRECTORY
  match access-group name ACTIVE-DIRECTORY
class-map match-all NET-MGMT
  match access-group name NET-MGMT
class-map match-any SCAVENGER
 match protocol napster
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 	
class-map COS6
 match cos 6
class-map COS5
 match cos 5
class-map COS4
 match cos 4
class-map COS3
 match cos 3
class-map COS2
 match cos 2
class-map COS1
 match cos 1
class-map COS0
	class-map match-all MARKED_VOICE
	  match ip dscp ef
	class-map match-any MISSION-CRITICAL
	  match ip dscp af41
	  match ip dscp af31
	  match ip dscp af21
	  match ip dscp af11
	  match ip dscp cs6
	  match ip dscp cs3
	  match ip dscp cs2
	class-map match-any SCAVENGER
	  match ip dscp cs1
	class-map match-any DEFAULT
	 match ip dscp cs0
	
	policy-map TIER-1.2-WAN-OUT
	  class MARKED_VOICE
	  priority percent 33
	  class MISSION-CRITICAL
	  bandwidth percent 41
	  random-detect dscp-based
	  class SCAVENGER
	  bandwidth percent 1
	  class DEFAULT
	  bandwidth percent 25
	  random-detect
	
	Interface <STRATEGIC WAN>
	  bandwidth <bandwidth>
	  service-policy output TIER-1.2-WAN-OUT

```
 match cos 0

policy-map COS-TO-DSCP
 class COS6
    set ip dscp cs6
 class COS5
    set ip dscp EF
 class COS4
    set ip dscp AF41
 class COS3
    set ip dscp AF31
 class COS2
    set ip dscp AF21
 class COS1
    set ip dscp AF CS1
 class COS0
    set ip dscp 0

class-map DSCP-CS6
 match ip dscp cs6
class-map DSCP-EF
 match ip dscp ef
class-map DSCP-AF41
 match ip dscp af41
class-map DSCP-AF31
 match ip dscp af31
class-map DSCP-AF21
 match ip dscp af21
class-map DSCP-CS11
 match ip dscp cs11
class-map DSCP-0
 match ip dscp 0

policy-map DSCP-TO-COS
 class DSCP-CS6
    set cos 6
 class DSCP-EF
    set cos 5
 class DSCP-AF41
    set cos 4
 class DSCP-AF31
    set cos 3
 class DSCP-AF21
    set cos 2
 class DSCP-CS1
    set cos 1
 class DSCP-0
    set cos 0

policy-map TIER-1.2-INGRESS
  class VOICE
```

```
    set ip dscp ef
  class DCTS
    set ip dscp af41
  class GCCS
    set ip dscp af31
  class C2PC
    set ip dscp af31
  class CUSTOM1
    set ip dscp af21
  class CUSTOM2
    set ip dscp af11
  class BGP-ROUTING
    set ip dscp cs6
  class VOICE-SIGNALING
    set ip dscp cs3
  class ACTIVE-DIRECTORY
    set ip dscp cs2
  class NET-MGMT
    set ip dscp cs2
  class SCAVENGER
    set ip dscp cs1
  class DEFAULT
    set ip dscp cs0

ip access-list extended VOICE
  permit udp <VoSIP/VoIP IP> any range 16384 32767
ip access-list extended DCTS
 permit  tcp <DCTS Svr IP> eq 80 any
 permit tcp <DCTS Svr IP> eq 8080 any
 permit tcp <DCTS Svr IP> eq 1503 any
 permit tcp <DCTS Svr IP> eq 1720 any
 permit tcp <DCTS Svr IP> eq 7640 any
 permit tcp <DCTS Svr IP> eq 7648 any
 permit udp <DCTS Svr IP> eq 7648 any
 permit udp <DCTS Svr IP> eq 24032 any
 permit udp <DCTS Svr IP> eq 56800 any

*Above is for server to server connections.  If client to
server details are required, please contact J6-CNE.

ip access-list extended GCCS
 permit tcp any any eq 9119
 permit tcp any any eq 9981
 permit tcp any eq 9119 any
 permit tcp any eq 9981 any
ip access-list extended C2PC
 permit udp any any eq 2000
 permit udp any any eq 2701
 permit udp any any eq 2702
ip access-list extended CUSTOM1
 permit TCP any any eq xxxx
```

ip access-list extended CUSTOM2 permit TCP any any eq xxxx ip access-list extended BGP-ROUTING permit TCP any any eq 179 ip access-list extended VOICE-SIGNALING permit tcp any any range 2000 2002 permit tcp any any eq 1720 permit tcp any any range 11000 11999 permit udp any any eq 2427 ip access-list extended ACTIVE-DIRECTORY permit udp any any eq 88 permit udp any any eq 389 permit udp any any eq domain permit tcp any any eq 3268 ip access-list extended NET-MGMT permit udp any eq 161 any permit udp any eq 9995 any permit udp any eq 9996 any Interface <1.2 LAN EDGE> Service-policy input TIER-1.2-INGRESS Interface <1.2 IDS INTFC> service-policy input COS-TO-DSCP service-policy output DSCP-TO-COS	

EXHIBIT 3 Tier-1/1 Configuration Example



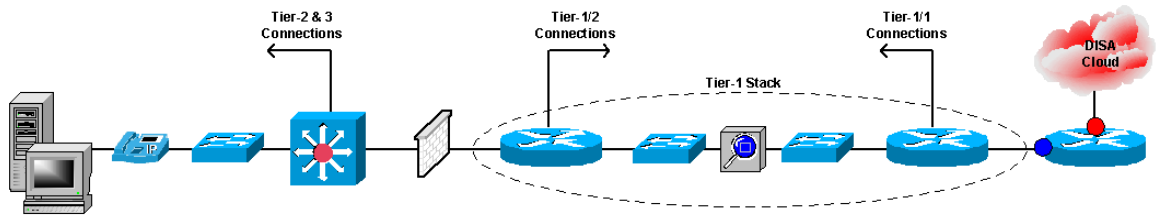
Tier-1/1: Queue

```
class-map match-all VOICE
  match ip dscp ef
class-map match-any MISSION-CRITICAL
  match ip dscp af41
  match ip dscp af31
  match ip dscp af21
  match ip dscp af11
  match ip dscp cs6
  match ip dscp cs3
  match ip dscp cs2
class-map match-any SCAVENGER
  match ip dscp cs1
class-map match-any DEFAULT
 match ip dscp cs0

class-map COS6
 match cos 6
class-map COS5
 match cos 5
class-map COS4
 match cos 4
class-map COS3
 match cos 3
class-map COS2
 match cos 2
class-map COS1
 match cos 1
class-map COS0
 match cos 0

policy-map COS-TO-DSCP
 class COS6
    set ip dscp cs6
 class COS5
    set ip dscp EF
 class COS4
    set ip dscp AF41
```

```
 class COS3
    set ip dscp AF31
 class COS2
    set ip dscp AF21
 class COS1
    set ip dscp AF CS1
 class COS0
    set ip dscp 0

class-map DSCP-CS6
 match ip dscp cs6
class-map DSCP-EF
 match ip dscp ef
class-map DSCP-AF41
 match ip dscp af41
class-map DSCP-AF31
 match ip dscp af31
class-map DSCP-AF21
 match ip dscp af21
class-map DSCP-CS11
 match ip dscp cs11
class-map DSCP-0
 match ip dscp 0

policy-map DSCP-TO-COS
 class DSCP-CS6
    set cos 6
 class DSCP-EF
    set cos 5
 class DSCP-AF41
    set cos 4
 class DSCP-AF31
    set cos 3
 class DSCP-AF21
    set cos 2
 class DSCP-CS1
    set cos 1
 class DSCP-0
    set cos 0

policy-map TIER-1.1-WAN-OUT
  class VOICE
    priority percent 33
  class MISSION-CRITICAL
    bandwidth percent 41
    random-detect dscp-based
  class SCAVENGER
    bandwidth percent 1
  class DEFAULT
    bandwidth percent 25
    random-detect
```

```
Interface <STRATEGIC WAN>
  bandwidth <bandwidth>
  service-policy output TIER-1.1-WAN-OUT

Interface <1.1 IDS INTFC>
 Service-policy input COS-TO-DSCP
 Service-policy output DSCP-TO-COS
```

EXHIBIT 4 **Tier-0 Configuration Example**



Tier-0: Mark & Classify	**Tier-0: Queue**

class-map match-all VOICE
  match access-group name VOICE
class-map match-all DCTS
  match access-group name DCTS
class-map match-all GCCS
  match access-group name GCCS
class-map match-all C2PC
  match access-group name C2PC
class-map match-all CUSTOM1
  match access-group name CUSTOM1
class-map match-all CUSTOM2
  match access-group name CUSTOM2
class-map match-all BGP-ROUTING
  match access-group name BGP-ROUTING
class-map match-all VOICE-SIGNALING
  match access-group name VOICE-SIGNALING
class-map match-all ACTIVE-DIRECTORY
  match access-group name ACTIVE-DIRECTORY
class-map match-all NET-MGMT
  match access-group name NET-MGMT
class-map match-any SCAVENGER
 match protocol napster
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 	
policy-map TIER-0-WAN-EDGE-IN
  class VOICE
  set ip dscp ef
  class DCTS
  set ip dscp af41
  class GCCS
  set ip dscp af31
  class C2PC
  set ip dscp af31
  class CUSTOM1
  set ip dscp af21
  class CUSTOM2
	class-map match-all MARKED_VOICE
	  match ip dscp ef
	class-map match-any MISSION-CRITICAL
	  match ip dscp af41
	  match ip dscp af31
	  match ip dscp af21
	  match ip dscp af11
	  match ip dscp cs6
	  match ip dscp cs3
	  match ip dscp cs2
	class-map match-any SCAVENGER
	  match ip dscp cs1
	class-map match-any DEFAULT
	 match ip dscp cs0
	
	policy-map TIER-0-WAN-OUT
	  class MARKED_VOICE
	  priority percent 33
	  class MISSION-CRITICAL
	  bandwidth percent 41
	  random-detect dscp-based
	  class SCAVENGER
	  bandwidth percent 1
	  class DEFAULT
	  bandwidth percent 25
	  random-detect
	
	Interface <STRATEGIC WAN>
	  bandwidth 3096
	  service-policy output TIER-0-WAN-OUT

```
    set ip dscp af11
  class BGP-ROUTING
    set ip dscp cs6
  class VOICE-SIGNALING
    set ip dscp cs3
  class ACTIVE-DIRECTORY
    set ip dscp cs2
  class NET-MGMT
    set ip dscp cs2
  class SCAVENGER
    set ip dscp cs1
  class DEFAULT
    set ip dscp cs0

ip access-list extended VOICE
  permit udp any <VoSIP/VoIP IP> range 16384 32767
ip access-list extended DCTS
 permit  tcp any eq 80 <DCTS Svr IP>
 permit tcp any eq 8080 <DCTS Svr IP>
 permit tcp any eq 1503 <DCTS Svr IP>
 permit tcp any eq 1720 <DCTS Svr IP>
 permit tcp any eq 7640 <DCTS Svr IP>
 permit tcp any eq 7648 <DCTS Svr IP>
 permit udp any eq 7648 <DCTS Svr IP>
 permit udp any eq 24032 <DCTS Svr IP>
 permit udp any eq 56800 <DCTS Svr IP>

*Above is for server to server connections.  If client to
server details are required, please contact J6-CNE.

ip access-list extended GCCS
 permit tcp any any eq 9119
 permit tcp any any eq 9981
 permit tcp any eq 9119 any
 permit tcp any eq 9981 any
ip access-list extended C2PC
 permit udp any any eq 2000
 permit udp any any eq 2701
 permit udp any any eq 2702
ip access-list extended CUSTOM1
 permit TCP any any eq xxxx
ip access-list extended CUSTOM2
 permit TCP any any eq xxxx
ip access-list extended BGP-ROUTING
 permit TCP any any eq 179
ip access-list extended VOICE-SIGNALING
 permit tcp any any range 2000 2002
 permit tcp any any eq 1720
 permit tcp any any range 11000 11999
 permit udp any any eq 2427
ip access-list extended ACTIVE-DIRECTORY
```

permit udp any any eq 88 permit udp any any eq 389 permit udp any any eq domain permit tcp any any eq 3268 ip access-list extended NET-MGMT permit udp any eq 161 any permit udp any eq 9995 any permit udp any eq 9996 any Interface <WAN EDGE> Service-policy input TIER-0-WAN-EDGE-IN	

References

a. Title 18USC2511, (USC 18 - Crimes and Criminal Procedure, Part 1 – Crimes, Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications Sec. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited), 26 January 1998.

b. DOD Dir 8500.2, Information Assurance Implementation (IA), 6 February 2003.

c. DOD Dir 8570.1, Information Assurance, October 24, 2002.

d. DOD Inst 8551.1, Ports, Protocols, and Services Management (PPSM), 13 August 2004

e. DOD 8510.1M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, 31 July 2000.

f. DOD Global CONOPS for Combined Regional Information Exchange System (CENTRIXS), 20 July 2004

g. CJCSI 6510.01D Information Assurance (IA) and Computer Network Defense (CND), 15 June 2004.

h. CJCSI 6511.01 Information Security Guidelines for the deployment of deployable switched systems, 1 February 2001.

i. CJCSI 6511.02B Defense Information System Network (DISN): Policy, Responsibilities, and Processes, 31 July 2003.

j. CJCSM 6231.07C, Manual for Employing Joint Tactical Communications, Joint Network Management And Control, 1 August 2001.

k. CJCSM 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), 25 Mar 03, CH1 10 Aug 04

l. CCR 25-206 Appendix E, USCENTCOM Information Systems Security (INFOSEC) Security Standards, -DRAFT- Jan 2004.

m. USCENTCOM Directorate of C4S, DRAFT Quality of Service (QoS) Policy Ver. 2.1, 8 Aug 2005

n. NSTISSI 7003, Protected Distribution Systems (PDS), 13 Dec 1996

o. NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, MIS Training Institute, January 2002.

p. Defense Information Systems Agency, DISA Global Contingency and Exercise Planning (CONEX) Guide 01-2003, Annex D (ITSDN SIPR NIPR)

This page intentionally left blank.