SIPRNET

CUSTOMER CONNECTION PROCESS GUIDE

14 February 2002

DISN Network Services/NS52
5275 Leesburg Pike
Falls Church, Virginia 22041

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2/14/2002	Report 2/14/2002

4. TITLE AND SUBTITLE
SIPRNET Customer Connection Process Guide

5. FUNDING NUMBERS

6. AUTHOR(S)
Alvarez, Joe

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Information Systems
Agency
DISN Network Services/NS52,
5275 Leesburg Pike, Falls
Church, VA 22041

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

Details on the SIPRNET connection process.

14. SUBJECT TERMS
IATAC Collection, SIPRNET

15. NUMBER OF PAGES
73

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

There are three major efforts a customer must be concerned with to obtain direct SIPRNET connectivity. These are identified within this document and are as follows:

Initial Modeling Request – Found on page 14
If Contractor or Non-DOD – Validation – Found on page 20
Security Accreditation Documentation – Found on page 50

These items are explained more thoroughly further on within the instructions.

SIPRNET Points of Contact:

Program Manager:

Mr. Joe Alvarez- 703-882-0190 (DSN: 381) / NS52

Classified Networks Customer Service Manager:

Mr. Jim Nostrant - 703-882-0191 (DSN: 381) / NS52 - nostranj@ncr.disa.mil

Customer Service Representative - Navy

Mr Johnnie (Jay) Johnson – 703-882-0195 (DSN: 381) / NS52 – johns10j@ncr.disa.mil

Customer Service Representative – Army / USAF

Ms. Candace Macisco– 703-882-1956 (DSN: 381) / NS52 – maciscoc@ncr.disa.mil

SIPRNET Security Manager:

Mr. John Staples - 703-882-2116 (DSN: 381) / NS52 – staplesj@ncr.disa.mil
(Security Accreditation Packages)

Joint Staff / J6T

Lt Col David Uhrich– 703-697-4503 (DSN: 227) David.uhrich@js.pentagon.mil

Waivers:

Ms Betty Lewis – 703-882-0215 (DSN: 381) - D3Waive@ncr.disa.mil

For problem reporting and opening up of trouble ticket for CONUS connections, once requirement has been declared operational please contact the Network Operations Center (NOC) at one of the following numbers:

1-800-451-7413 - 1-703-692-8481 / 8482

NOTE

We have had occasions operational customer locations where particular sites determine that they would, for one reason or another, wish to have the host equipment moved. Users locations must remember that they are NOT to move DISA owned equipments. This includes, but is not necessarily limited to, Encryption deices, CSU/DSUs, and on occasion, line drivers/repeaters. If site wishes to

move their location they are to submit RFS through their normal chain of command. In the past sites have indicated they had the expertise to do a move and invariably there would be a problem. In addition, when moving from site identified in the Security Accreditation documentation to another could nullify the accreditation.

SIPRNET ACCESS CHECKLIST:

To ensure you are able to obtain connectivity to the SIPRNET please complete the following checklist as you go through the process.

Have you contacted the SIPRNET PROGRAM MGMT OFFICE? (In the event you received this checklist without the remainder of the SIPRNET CUSTOMER CONNECTION PROCESS) Yes / No

CONTRACTORS ONLY – Has your Sponsor contacted Joint Staff regarding validation of your requirement To have connectivity to SIPRNET? Yes / No

NON DOD ONLY – Have you contacted Joint Staff Regarding validation of your requirement to have Connectivity to SIPRNET? Yes / No

CONTRACTOR ONLY – Have you been in contact with Defense Security Services (DSS) regarding Security Accreditation Package? Yes / No

Have you submitted Initial Modeling Request (IMR) to SIPRNET to obtain "B" Side information for your connection? Yes / No

Have you received "B" Side information back from SIPRNET office? Yes / No

Have you, or your Sponsor in the case of Contractor Connections, submitted Request For Service (RFS) To your supporting Telecommunications Certification Office? Yes / No

Have you, with the exception of contractor connections which go through DSS, submitted Security Accreditation Package to SIPRNET? Yes / No

Has Telecommunications Service Request been Issued for you requirement? Yes / No

Has Telecommunications Service Order (TSO) been Issued for your requirement? Yes / No

Do you have customer premis equipment for connection to the SIPRNET? Yes / No

Have you obtained backside IP Addresses from SIPRNET SUPPORT CENTER? (If Applicable) Yes / No

SIPRNET CUSTOMER CONNECTION PROCESS

1. Initially the customer will contact Mr. Jim Nostrant , Mr Jay Johnson or Mr Joe Alvarez to obtain information regarding the SIPRNET and procedures for connection to the Network.

If the customer requirement is outside the continental United States (CONUS) there is no requirement for customer to contact above. Simply submit "A" Side only RFS to their supporting Telecommunications Certification Office (TCO). TCO will then submit "A" Side only Telecommunications Service Request (TSR) directly to DISA-Europe or DISA-Pacific respectively. In other words, initial modeling is not required. All Security requirements and documentation are still required.

2. As the primary customer contact for SIPRNET customers, Mr Jim Nostrant will be POC for SIPRNET connectivity.

3. During initial conversation with customer, arrangements should be made to provide the customer the current information package. At present it consists of the following.

A. Current billing rates for connectivity.
B. Information pertaining to the Security Accreditation Package which customer needs to complete and return. It should be noted that this is not a sample Security Package.
C. Initial Modeling Request form.

4. When speaking with the customer SIPRNET personnel must ensure customer understands specific items relating to connectivity to the SIPRNET. These must consist of, but are not limited to the following:

A. There is an approximate 150 day lead time from date TSR issued prior to connectivity to the network.

1. There are individuals within the organization who advocate approximately 30 days. This is a valid goal but at this juncture it is simply not possible on a regular basis.

2. Effective immediately connections WILL NOT be activated until such time as an IATC has been issued by NS52. Connection will be made as normal but will not be activated. In addition, customer may be billed for connectivity effective this date. Exceptions to this will be on a case by case basis through the J6.

a. Customer must allow a minimum of 60 days for evaluation of submitted security package prior to intended activation date.

B. Requirement for site survey, (normally done by contractor) of host location.

1. Customer location site survey is normally NOT done.

2. There are, in fact, some locations, although very few, which could possibly require a site survey.

3. Due to scheduling requirements those locations requiring a survey may have delay in implementation and incurred cost may be passed to the customer.

C. Requirement of customer to coordinate with their specific COMSEC Custodian for issuance and delivery of KIVs or KGs and keying material to host location. Customer needs to remember that the fill device for a KG-194 is a FIREFLY fill device DISA provides while a KIV-7HS is a KOI-18. The customer needs to coordinate with their local COMSEC Custodian to ensure they have the appropriate fill device before circuit can be activated. This IS NOT provided by DISA.

1. This is to be completed so Crypto Equipment and keying material will be on site prior to FE visit for installation. DISA WILL PROVIDE the required KIVs or KGs and CSU/DSUs based on speed requirements.

a. **64KB or less the general rule of thumb will be KG-84 with CODEX CSU/DSU at user location.**

b. **128kb or above would be KIV-7HS supported by Larscom CSU/DSUs**

D. Requirement for customer to complete installation of their host equipments. DISA (Contractor Support) is only required to complete installation up too the Red side of KIV/KG. Cabling and connectivity from Red side KG to host equipment is the responsibility of the customer.

1. Host hardware and software is to be installed prior to visit by contractor to actually complete installation to the SIPRNET. At least to the extent that connection can be tested. In this fashion DISA will eliminate the frequency of multiple visit to same location at various stages of the activation. Customers must also understand that DISA does not provide customer Premise routers. Majority of existing customers have connected some type of router to the SIPRNET. Those that elect to connect other equipments such as workstations etc must realize that whatever equipments they elect to connect must support TCP/IP.

E. For Ethernet or Fast Ethernet type connections it is the responsibility of the customer to provide and install cabling up to the SIPRNET Hub router. Field Engineer will normally not be sent on these installation/activations. Customer must remember that this Ethernet path is Red and must be protected as such.

F. Network Delay - There is a 150 millisecond delay one way within theatre incurred on the SIPRNET or 300 millisecond round trip. When going between theatres such as a connection from Europe to CONUS this number would be 300 milliseconds one way (600 roundtrip). This is a worst case scenario.

G. All customers must be DOD Government Service or Agency. Any private contractor connections must be sponsored by a DOD government service or agency. (See Item 11) In addition, contractors are not to be backsided to DOD Service or Agency SIPRNET Host equipments..

1. Network connections of Non DOD Government Agency or contractor sites must be validated through J6. For contractor requirements the sponsoring Service or Agency has the responsibility of contacting J6. The J6 point of contact is LtCol Uhrich at (comm) 703-697-4503 (DSN) 227

2. Contractor connections must also go through the Defense Security Service, DSS, for accreditation of their facilities. This is to include direct connections to the SIPRNET.

H. Depending upon the type of connection and the number of "backside hosts", the customer may or may not be required to obtain an Autonomous System Number (ASN). This can be determined by contacting the SIPRNET Support Center (SSC) 1-800-582-2567 / 1-703-821- 6260. If needed, the customer can obtain an ASN by going thru the SSC.

I. Requirement for customer to provide the "backside" IP address. We will provide the network address (e.g., 140.049.XXX.XXX) for the actual connection to the network. It is the customers responsibility to obtain/provide the addressing to the backside of their premise equipments. This is required prior to being able to activate the connection. If customer does not already have these addresses they may be obtained from the SIPRNET Support Center.

****NOTE** ALL BACKSIDE IP ADDRESSES UTILIZED ON THE SIPRNET MUST BE REGISTERED WITH THE SIPRNET SUPPORT CENTER. NIPRNET IP ADDRESS ARE NOT AUTHORIZED FOR USE ON THE SIPRNET.**

a. **The exception to this rule are those connections to a contractor facility. To obtain their backside IP Addresses contractor sites must contact Mr James Jones or Mr Larry Moore at disn@mail.dss.mil**

J. Specific items related to obtaining circuit path to customer locations. On numerous installations it has been found that the most difficult portion of the connection becomes the last 50 feet. This is normally from the commercial demarcation point to the host. Ie: the local GFE path. In some instances this is a contractor supported/maintained path with site specific methods for completion. We need to know of potential problems associated with the completion of this portion of the connection. This would include a local POC at the base/camp or station who should be coordinated with in the TSR/TSO process. This information could very well be the difference between a successful completion and an extended delay.

K. There are specific differences between customer requirement of T1/E1 1.544MB/2.048MB and below and those of a greater bandwidth and not collocated with an existing SIPRNET Node. DISA will pay for access circuits for customer requirements which are equal to or less than T1/E1, 1.544MB/2.048MB originating in an area not identified as meet me billing. For requirements of a greater bandwidth customer may be responsible for funding for access circuits. This will be determined once Configuration Management has determined the method of connectivity for a particular requirement. In either case DISA will continue to provide the encryption equipment. In addition, for these type connections Ethernet wi ll not be an option.

5. When the customer returns the completed Initial Modeling form to NS52 the following actions will occur.

A. SIPRNET personnel sends E-Mail request to modeling function to determine the following.

1. **SIPRNET Hub to which customer connection will be made.**
2. **IP Address assigned to customer. ie: 140.049.XXX.XXX**

6. Once modeling provides items 1 and 2 back this information is passed to the customer. This should normally be within 72 hours of receipt of Initial Modeling Effort form from customer.

7. Customer submits Request For Service (RFS) to their respective supporting Telecommunications Certification Office (TCO) for the issuance of the Telecommunications Service Request (TSR).

Please ensure the following PLA address is included when sending RFS.
(gsi-ncro@ncr.disa.mil)

****IMPORTANT****

TO ENSURE REQUIREMENT IS PROCESSED PROMPTLY PLEASE CONTACT JIM NOSTRANT AS SOON AS RFS IS RELEASED.

A. As this is an encrypted Network when submitting RFS customer MUST remember to include COMSEC information.

1. **COMSEC Account Number**
2. **COMSEC Custodian=s Name**
3. **COMSEC Custodian=s Phone Number**
4. **PLA for Comsec Custodian**
5. **Mailing Address for COMSEC Custodian**

B. There are some slight variations within this process determined by supporting TCO:

1. Air Force has requested that all of their requirements go through the Air Force Systems Networking Program Office. (AFSN) at Gunter AFB. DISA will continue to work with customers as previously explained but customer is to send their request for B side information through the AFNSC.

POC is Captain John Morgan
Phone © 334-416-5769 (d) 596-5769
FAX is © 334-416-3325 (d) 596-3325
E-Mail: john.morgan@gunter.af.mil

2. US Marines – It has been requested that all of the US Marine requirements go through the following.

Mr Peter Pozeg
MITNOC
VOICE: 703-784-5182
FAX COMM: 703-784-4919/3477
DSN: 278
E-Mail: pozegpa@noc.usmc.mil

8. Upon receipt of Modeling information NS52 will notify customer of B side. This is the specifics as to which Hub and port assignments have been assigned against this connection requirement.

9. Upon receipt of TSR, NS52 knows funding has been applied to requirement. At this point it should be approximately 150 days for connectivity. Once TSO is received the requirement is actually placed on the Master Schedule for implementation/activation.

A. Regardless of ROD date identified, requirement will not be placed on Master Schedule any sooner than 8 weeks from date TSO received by support contractor. It takes up to 6 weeks to obtain keying material once TSO has been issued. If placed on Schedule for a date prior to arrival of key at customer location installation must be slipped thus disturbing the Master Schedule unnecessarily.

10. Once NS52 receives the customer's Security Accreditation documentation the following actions occur.

A. NS52 will review documentation for accuracy and completeness.

B. After a determination that the minimum connection requirements have been met, NS522 will issue an IATC and the connection can be made.

C. NS522 will perform an on-line compliance assessment

D. Upon successful completion of the compliance assessment and connection documentation requirements, NS522 will issue a Final Approval to Connect.

11. FOREIGN NATIONAL CONNECTIVITY - (See Information Paper)

12. SIPRNET SUPPORT CENTER - 1-800-582-2567 / (703) 676-1050

13. SIPRNET RATES:

ALL THEATRES IP ROUTER SERVICE - MONTHLY RECURRING CHARGES / FY00

BANDWIDTH	CONUS	PACIFIC (AK & HI)	EUROPE	WESTPAC
64kb/Below	$405	$405	$600	$700
128kb	$709	$709	$1,049	$1,225
256kb	$1,215	$1,215	$1,799	$2,100
384kb	$1,620	$1,620	$2,389	$2,801
512kb	$2,025	$2,025	$2,998	$3,501
768-896kb	$2,228	$2,228	$3,298	$3,851
1 MBPS	$2,329	$2,329	$3,448	$4,026
1.024-1.544 MBPS	$2,430	$2,430	$3,598	$4,201
2-2.048 MBPS	$2,532	$2,532	$3,748	$4,376
3 MBPS	$2,633	$2,633	$3,898	$4,551
4 MBPS	$2,937	$2,937	$4,347	$5,076
5 MBPS	$3,241	$3,241	$4,797	$5,601
ETHERNET 6MBPS	$3,646	$3,646	$5,397	$6,301
7 MBPS	$4,051	$4,051	$5,996	$7,001

8 MBPS	**$4,253**	**$4,253**	**$6,296**	**$7,352**
9 MBPS	**$4,658**	**$4,658**	**$6,896**	**$8,052**
12 MBPS	**$5,874**	**$5,874**	**$8,695**	**$10,152**
15 MBPS	**$6,846**	**$6,846**	**$10,134**	**$11,832**
18 MBPS	**$8,102**	**$8,102**	**$11,992**	**$14,003**
21 MBPS	**$9,114**	**$9,114**	**$13,491**	**$15,753**
24 MBPS	**$10,410**	**$10,410**	**$15,410**	**$17,994**
27 MBPS	**$11,869**	**$11,869**	**$17,569**	**$20,514**
30 MBPS	**$13,165**	**$13,165**	**$19,488**	**$22,755**
33 MBPS	**$14,461**	**$14,461**	**$21,406**	**$24,995**
36 MBPS	**$16,568**	**$16,568**	**$24,525**	**$28,636**
39 MBPS	**$18,877**	**$18,877**	**$27,942**	**$32,627**

***56KB AVAILABLE IN CONUS, 64KB FOR O'CONUS CONNECTIVITY.**

****NON RECURRING CHARGES FOR INSTALLATIONS:**

$2,500 for < 512KBS
$5,000 for > 512KBS <= 2.048 MB
$12,000 for 3MB <= 45MB
$15,000 for >45MB

***** DIAL-UP SERVICE = $50 INITIATION FEE PLUS $27 PER MONTH PER COMM SERVER ACCESS CARD.**

*****THE MANAGEMENT OF CUSTOMER PREMISE ROUTERS (CISCO OR WELLFLEET ROUTERS) HAVE A FLAT FEE OF $50.00 PER MONTH . ALL OTHER ROUTER MANAGEMENT (NOT CISCO OR WELLFLEET) WILL REQUIRE A SPECIFIC COST ESTIMATE TO DETERMINE A FEE.**

******DISA DOES NOT BILL CONTRACTORS. CONTRACTOR CONNECTIONS MUST BE SPONSORED AND SERVICE OR AGENCY SPONSOR IS RESPONSIBLE TO DISA FOR THE BILL.**

*******ADDED TO THE ABOVE RATES THERE MAY BE A 7.9% SURCHARGE.**

FOR CUSTOMER REQUIRMENTS ABOVE THE T1/1.544MB RATE PLEASE BE SURE TO COORDINATE WITH PROGRAM MANAGEMENT OFFICE REGARDING DISTANT END REQUIREMENT FOR CONNECTIVITY. WHERE WE ARE IN THE PROCESS OF UPGRADING THE BACKBONE TO DS3 FROM T1 IN NUMEROUS LOCATIONS, IT MAY NOT BE TO A SPECIFIC LOCATION YOU WISH TO COMMUNICATE WITH. BY IDENTIFYING THE DISTANT END POINTS DURIG INITIAL MODELING THE BACKBONE MAY BE ENHANCED TO SUPPORT YOUR END TO END REQUIREMENT. PLEASE BE ADVISED THAT IF IN FACT THERE IS A HIGH BANDWIDTH REQUIREMENT FOR CONNECTIVITY END TO END THAT, AS IN ANY OTHER CONNECTION, THIS IS ESSENTIALY 2 SEPARATE CONNECTIONS TO THE NETWORK.

MEET ME BILLING RATES HAVE BECOME FURTHER DEFINED AS TO WHAT LOCATIONS WITHIN THE EUROPEAN AND PACIFIC THEATRES THE FLAT RATE CONNECTION CHARGES WILL BE APPLIED TO. FOR THOSE AREAS NOT IDENTIFIED BELOW, MEET ME BILLING WILL APPLY. MEET ME BILLING IS WHERE THE CUSTOMER IS RESPONSIBLE FOR THE COST OF ACCESS CIRCUIT TO THE DISN NODE PLUS THE RATE FOR THE ORDERED DISN SERVICE. (CONNECTION CHARGE) ADOPTING A "MEET ME BILLING" APPROACH IS A FUTURE STEP IN ADOPTION OF COMMERCIAL TYPE BILLING FOR THE DISN SERVICES AS MANDATED BY ASD(C3I) AND USD(C).

EUROPEAN RATES:

AZORES
BELGIUM
BOSNIA
GERMANY
ICELAND
ITALY
SPAIN

TURKEY
UNITED KINGDOM

PACIFIC RATES:

AUSTRALIA
GUAM
DIEGO GARCIA
JAPAN
OKINAWA
KOREA

MEET ME BILLING WILL APPLY TO OUR SERVICES ORDERED WHICH EXTEND TO COUNTRIES OUTSIDE OF THE THEATRES DEFINED ABOVE.

14. BACKSIDE CONNECTIVITY

The following message is referring to those local connections to the backside of a SIPRNET customer' host. For example, a host front end to a base Red LAN. Those on base connections would be acceptable but off base connectivity would not normally be allowed.

ROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINE ROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINEROUTINE

R 121734Z AUG 97

FM DISA WASHINGTON DC//D3//

TO DISA WASHINGTON DC//D3//
HQ USAF WASHINGTON DC//SCM//
CMC WASHINGTON DC//C21/POC-30/C412//
HQDA WASHINGTON DC//SAIS-C4X//
CNO WASHINGTON DC//OP941/N61/N62//
NIMA HQ FAIRFAX VA//TSC//
HQ DNA WASHINGTON DC//NOCC//
DIA WASHINGTON DC//DS/CISA/SYS//
DLA FT BELVOIR VA//CAN//
DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y44/CIO//
NRO WASHINGTON DC//COM//
ONI WASHINGTON DC//O7//
DECA FT LEE VA//
SECDEF WASHINGTON DC//BMSO/USDP-DSAA/ASD-GC//
USCINCTRANS SCOTT AFB IL//TCJ6/USTC/J2-PY//
CINCUSACOM NORFOLK VA//J63/ACJ6//
USCINCEUR VAIHINGEN GE//ECJC//
USCINCSTRAT OFFUTT AFB NE//J6//
USCINCSO SCJ1 QUARRY HEIGHTS PM//
USCINCSPACE PETERSON AFB CO//J6//
USCINCCENT MACDILL AFB FL//J6//
USCINCSOC MACDILL AFB FL//J6//
USCINCPAC HONOLULU HI//J6//
JOINT STAFF WASHINGTON DC//J6T//
SECDEF WASHINGTON DC//C3I//
CDRUSAIC FT HUACHUCA AZ//STZS-IMI-T//
HQ AFCIC WASHINGTON DC//SYN//
AFPCA WASHINGTON DC//SMT//
PEOCMPANDUAV WASHINGTON DC//PEOCU-B22//
HQ SSG MAXWELL AFB GUNTER ANNEX AL//SIN/SCMGU//
NCTAMS LANT NORFOLK VA//N3/N33/N33D/N33N/12//
DRPC PAC PEARL HARBOR HI//PCR34//
NCTAMS EASTPAC HONOLULU HI//N34//
CDROPMAS-E DCS STA LANDSTUHL GE//ASQE-F-ITT-LDL//
CDR5THSIGCMD RFS-TSR TFC MANNHEIM GE//ASQE-OP-SCC//
MARCORCOMTELACT QUANTICO VA//
NAVCOMTELSTA SAN DIEGO CA//
NTCC CAMP H M SMITH HI//
DISA WASHINGTON DC//COS/D2/D35/D36/D5/D6/D7/D8//
DISA PAC WHEELER AAF HI//PC2/PC21/PC31//
DISA EUR VAIHINGEN GE//EU2/EU3/EU21//

DMC COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//
DISA CENTRAL COMMAND FWD//JJJ//
DISA FLD OFC FT MCPHERSON GA//SANM//
DISA FIELD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA FT HUACHUCA AZ//JJJ//
DISA CENTRAL COMMAND MACDILL AFB FL//
DISA-PAC ELMENDORF AFB AK//

UNCLAS
REQUEST WIDEST DISSEMINATION OF THIS MESSAGE TO YOUR SUBORDINATE ORGANIZATIONS//

MSGID/GEN ADMIN/D36/AUG/97//

SUBJ/GUIDANCE FOR COMPLYING WITH ASD(C3I) POLICY, 5 MAY 97, MANDATING USE OF DEFENSE INFORMATION SYSTEMS NETWORK (DISN) OR FTS COMMON USER TELECOMMUNICATIONS SERVICES//

NARR/1. OFFICE OF THE ASST SECRETARY OF DEFENSE FOR C3I ISSUED 5 MAY 97 POLICY MEMORANDUM TO CLARIFY AND REINFORCE EXISTING POLICY MEMORANDUM (4640-13 AND 4640-14) MANDATING DOD USE OF DISN COMMON-USER SERVICE AND FTS. MEMO DIRECTS DISA TO PUBLISH PROCEDURES AND CRITERIA FOR REVIEWING REQUESTS FOR EXCEPTION TO USE DISN AND FTS. THIS MESSAGE PROVIDES INTERIM GUIDANCE FOR COMPLYING WITH SAID POLICY.

2. IAW ASD(C3I) POLICY, ALL DOD LONG-HAUL TELECOMMUNICATIONS REQUIREMENTS WILL BE SATISFIED BY DOD COMMON-USER DISN OR BY FTS 2000/2001. LONG-HAUL TELECOMMUNICATION SERVICES ARE ANY AND ALL INTERSITE (ENTERING OR LEAVING CONFINES OF POST, CAMP, STATION, BASE, INSTALLATION HEADQUARTERS, OR FEDERAL BUILDING) VOICE, DATA, AND VIDEO SWITCHING AND TRANSMISSION SERVICES AND ASSOCIATE NETWORK MGMT, TO INCLUDE REGIONAL SERVICES, METROPOLITAN AREA NETWORKS (MANS), AND ASYNCHRONOUS TRANSFER MODE EDGE DEVICES.

3. EFFECTIVE IMMEDIATELY, ANY DOD LONG-HAUL NETWORK OR CIRCUIT (EXISTING, NEW, OR UPGRADE) MUST BE COMPLIANT WITH THIS POLICY. IF NOT COMPLIANT, YOU MUST SUBMIT TO DISA A REQUEST FOR EXCEPTION TO THE 5 MAY 97 POLICY. DISA, AS THE MANAGER/SOLE PROVIDER OF LONG-HAUL AND REGIONAL TELECOMMUNICATION SERVICES, WILL ASSESS YOUR REQUEST AND ISSUE A WAIVER TO POLICY. WAIVERS WILL BE GRANTED ONLY UNDER EXTRAORDINARY CIRCUMSTANCES WHERE AN INITIATIVE OR REQUIREMENT CANNOT AT THIS POINT IN TIME BE TECHNICALLY OR ECONOMICALLY SATISFIED BY DISN OR FTS.

4. SUBMIT REQUEST FOR EXCEPTION TO POLICY TO DISA D36, 701 COURTHOUSE ROAD, ARLINGTON, VA 22204-2199 OR EMAIL TO CENACJ@NCR.DISA.MIL. PROVIDE THE FOLLOWING INFORMATION:

A. REQUIREMENT/NAME/TYPE OF NETWORK OR SERVICE (NUMBER OF T1/3S

FROM PORT A TO PORT B, ABCNET, SECRET, ATM NETWORK, OR XYZNET, UNCLAS MAN). PROVIDE CUSTOMER BASE, CONTRACT VEHICLE, AND GEOGRAPHIC LOCATION(S) SERVED. IDENTIFY PRINCIPAL USERS SUPPORTED.

B. JUSTIFICATION/NARRATIVE INCLUDING GENERAL DESCRIPTION OF THE REQUIREMENT/NETWORK OR SERVICE, THE PROPOSED SOLUTION, AND AN EXPLANATION AS TO WHY DISN OR FTS COMMON-USER SERVICE CANNOT BE USED.

C. SUMMARY OF PLANS TO MIGRATE TO DISN OR FTS COMMON-USER SERVICE.

D. POINT OF CONTACT - NAME, ORGANIZATION, PHONE, EMAIL AND MAILING ADDRESS.

5. UPON RECEIPT OF REQUEST FOR EXCEPTION, DISA WILL MAKE AN INDEPENDENT ASSESSMENT OF THE TECHNICAL AND ECONOMIC FEASIBILITY FOR IMMEDIATE MIGRATION TO DISN OR FTS. DISA D36 WILL NOTIFY REQUESTING SERVICE/AGENCY WITHIN 30 DAYS OF ASSESSMENT RESULTS.

6. DISA POINT OF CONTACT IS MS JEAN CENAC, D36, (703) 735-8168 (DSN 653-8168), EMAIL: CENACJ@NCR.DISA.MIL.//

NOTE POC FOR WAIVERS AS BEEN CHANGED TO MS BETTY LEWIS AT 703-735-8168 (DSN) 653-8168, EMAIL: D3WAIVE@NCR.DISA.MIL

15. PREMISE ROUTER MANAGEMENT

A. The RCC will perform remote customer premise management for CISCO or Wellfleet routers connected directly to the SIPRNET. The fee for this service is $50.00 per month, per router. This service will be obtained via submission of a Telecommunications Service Request (TSR). The customer must include in line item 401 of the TSR request for this service, ie: Request DISA provide customer premise management of CISCO/Wellfleet router located at.....

B. Premise router management will only extend to the premise router equipment connected directly to a SIPRNET Hub router. Premise router management will not extend beyond the first premise router. This means access circuits beyond the customer premise router will not be managed as part of this service offering.

C. Network management services will consist of the following.

1. Router configuration table management, to include updating and reloading, activating protocols, configuring routers, and addressing. Note, DISA will provide initial configuration of customer premise routers, for those routers that can be configured remotely.

2. Remote fault isolation and troubleshooting of the customer premise router.

3. Restoration service, across the network, of hardware equipment and software configuration. Premise router maintenance is NOT included in this service offering.

D. It is the customers responsibility to ensure the DISA RCC receives router updates to their router configuration requirements and all premise router passwords necessary for network configuration management. The customer must be able to provide on site personnel, at the customer premise, to aid in remote fault isolation and troubleshooting. The DISA RCC is the only authorized agent to make premise router configuration changes. Therefore, only the RCC will have the second level password.

16. DIAL UP CONNECTIVITY

For those customers who do not feel they have a direct SIPRNET requirement and wish to utilize the dial up offering this can be obtained by contacting the SIPRNET Support Center. 1-800-582-2567 / 703-676-1050. It must be understood by the customer that the monthly recurring fee for dial up access is per access card and not per site. Currently contractor locations are not authorized dial-up type connectivity. Those requirements which are US Government, but Non DOD do not require a Sponsor but must go to Joint Staff with validation to obtain dial up access.

SIPRNET

(INITIAL MODELING REQUEST)

INFORMATION REQUIRED TO OBTAIN B SIDE INFORMATION

SYSTEM NAME_____
(Not SIPRNET)
CONTRACTOR Facility _____ YES_____NO_____
ASSOCIATED SERVICE/SPONSOR _____
(Army, Air Force, Navy, Specific Agency)
REQUIRED OPERATIONAL DATE_____
(Based on minimum lead time of 150 Days from TSR Receipt by his office)
SPEED_____

With those requirements above T1/1.544MB. Is this associated with multiple other connections or primarily communicating with a particular endpoint? If yes, who? Reason for this specific question is for the Program Management office to ensure sufficient bandwidth is available between separate endpoints within the backbone.

BUILDING_____
ROOM_____
SPECIFIC MAILING ADDRESS_____
_____
_____
EQUIPMENT_____
(That which is connecting directly to SIPRNET HUB router)
ATM CELL Based_____IP Based

Primary POC_____
PHONE (comm)_____(dsn)_____
USERs ORGANIZATION_____
USERs ORGANIZATIONAL E-MAIL ADDRESS_____

Alternate POC_____
PHONE (comm)_____(dsn)_____
USERs ORGANIZATION_____
USERs ORGANIZATIONAL E-MAIL ADDRESS_____

(At host connection location, not Headquarters)

Commercial Demarcation Point (DEMARC)(This is the location where commercial circuitry vendors normally terminate their connection.)

Building_____
Room_____
POC_____
Phone_____

SITE COMM PERSONNEL_____
(ie: Base Comm Office, if available)
PDC_____
(Program Designator Code) (If this is not immediately available place To Be Determined on form. It is not critical at this point but must be included in RFS/TSR)

-- SAMPLE RFS --

FM DISA WASHINGTON DC//D343//
TO (Your appropriate TCO support, DCO-SCOTT, DCO-NCR, etc;)
INFO DISA WASHINGTON DC//D343/D345//

MESSAGE ADDRESSES OF STATIONS AT THE USER LOCATION AND WITHIN YOUR COMMAND/AGENCY WHO WILL HAVE TO TAKE ACTION ON THIS RFS

*****NOTE: (P) = PERMANENT, THE INFORMATION CONTAINED IN THESE ITEMS SHOULD ALWAYS BE THE SAME. PLEASE ENSURE THAT YOU REMOVE ALL THE (P) BEFORE YOU SUBMIT YOUR RFS.**

BT
UNCLAS
SUBJ: REQUEST FOR SERVICE
A. TSRE (DATADCS, LEASED, INTRA CONUS, DISN)
101. DATE AND YOUR RFS NUMBER (ie; RFS27FEB980001/2/3 etc;)
102. TSP # (Required if a CHANGE, AMEND or DISCONTINUE.
103. START (P) (Type action, START, CHANGE, Amend etc.)
104. CIRCUIT ONLY/SINGLE VENDOR - (P)
105. DISN ROUTER SERVICE - (P)
106A. 160001Z JAN 97 (DATE YOU WANT SERVICE) - (P)
106B. 160001Z JAN 97 (DATE YOU WANT SERVICE) - (P)
108. S7 - (P) (Purpose and use code)
109. 4G - (P) FOR 1.544MB, 4F FOR 0-64KB, 5A FOR 64KB TO 768KB, NS FOR 10MB
110. FULL DUPLEX - (P)
111. SPEED OF SERVICE YOU WANT, IE 64KB, 128KB, 512KB, 1.544KB
112. FULL PERIOD (P)
115. NO SIGNALING - (P)
116. NEW LEASE - (P)
117. YOUR PDC CODE
118. AMOUNT OF MONEY FOR OVERTIME AND EXPEDITE IF YOUR REQUEST IS UNDER 120 DAYS. (This only for payment of extra funds to commercial vendor.
Normal connections with the appropriate lead times do not require this field.)
119D. YES/ALL SATELLITE - (P) (Transmission media to be avoided) (If YES, Item #408 is required)
120A. FALCON (User location) GEOLOCO IF AVAILABLE
121A. 08 (State / Country code) IF KNOWN
122A. 1 (Area Code) IF KNOWN
123A. SPH-(P) (Facility Code) (SPH = SIPRNET Host / GCH = GCCS Host)
124A. BUILDING (To include street address)
125A. ROOM
126A. CISCO (ROUTER SERIES NUMBER, IE: 7500, 7000, ETC
127A. KIV-7HS
128A. DISA TO PROVIDE CSU/DSU. INTERFACE RS-530, V.35 etc. - (P)
129A. 4W-(P)
130A. USER POC NAME AND BOTH COMMERCIAL AND DSN PHONE NUMBERS. ONE ALTERNATE NAME AND PHONE NUMBER.
131A. COMPLETE ADDRESS (For user) (Mailing Address)
139A. NPANNX example: 703-735-3238 = my phone number

NPANNX = 703735

(There would be no break here. Only for this SAMPLE. B information will be provided by DISA D3113)
Once TSO is issued RFS must contain both "A" & "B" location information.

120B. HUB ROUTER LOCATION
121B. STATE/COUNTRY CODE
122B. SEE 122A
123B. SP1 - (P)
124B. BUILDING NUMBER (Where SIPRNET Hub is located)
125B. ROOM NUMBER
126B. TYPE OF TERMINAL EQUIPMENT
127B. KIV-7HS
128B. DISA TO PROVIDE CSU/DSU. INTERFACE RS-530 - (P)
129B. 4W - (P)
130B. HUB ROUTER POC NAME AND BOTH COMMERCIAL AND DSN PHONE NUMBERS. ALTERNATE NAME AND PHONE NUMBERS.
131B. COMPLETE ADDRESS (Mailing)
139B. AREA CODE/FIRST THREE NUMBERS OF PHONE NUMBER
353. SYSTEM ACRONYM – SYSTEM/PROJECT NAME
363. COMSEC ACCOUNT NUMBER
364. COMSEC CUSTODIAN - COMMERCIAL/DSN PHONE NUMBER
365. COMSEC CUSTODIAN MAILING ADDRESS
366. COMSEC CUSTODIAN PLA (Autodin) ADDRESS
401. RFS ISSUED TO PROVIDE, INSTALL, MAINTAIN A (SPEED OF CIRCUIT) CIRCUIT AND ASSOCIATED GFE EQUIPMENT BETWEEN SERVICE POINTS INDICATED, ALSO TO ESTABLISH TSP.
402. POC: YOUR NAME, ORGANIZATION, AND PHONE NUMBERS.
405. Y3 - (P)
408. JUSTIFICATION FOR SATELLITE OR OTHER EXCLUSION IDENTIFIED IN ITEM 119D.
410. COMMERCIAL VENDOR/TELCO BLDG/ROOM DEMARC POINT LOCATION TO INCLUDE STREET ADDRESS AND POC/PHONE NUMBER.
415B. SIPRNET
417. A. IF YOU HAVE ANY SPECIAL INSTALLATION REQUIREMENTS YOU WILL LIST THEM HERE. PLEASE INCLUDE YOUR SPECIFIC NAME WITHIN THIS BLOCK.
B. THE CIRCUIT VENDOR WILL TELEPHONICALLY CONTACT THE SITE POCs A MINIMUM OF 24 HOURS PRIOR TO ANY ONSITE INSTALLATION ACTIONS.
C. IF THE VENDOR IS UNABLE TO CONTACT SITE PERSONNEL CONTACT (YOUR NAME AND PHONE NUMBERS)
D. AUTHORIZATION FOR UTILIZATION OF THIS PDC IS AGAIN YOUR BOSS's NAME, ORGANIZATION, PHONE NUMBER. (HIS/HER SIGNATURE BLOCK)
E. THIS REQUIREMENT IS IN SUPPORT OF THE CLASSIFIED SIPRNET ROUTER NETWORK.
F. RFS POC: YOUR NAME AND PHONE NUMBERS
430. 60 MONTHS - (P) (How long do you need the connection? Normally not done longer than 60 or less than 12 months)
431. D - (P)
437A. CPIWI - (Yes/No) CPIWM - (Yes/No) (Do you want vendor to install and maintain the local circuit path from the commercial demarc to your location) (If yes, item 410A will be commercal demarc location.
437B. CPIWI - CPIWM -
438A. NONE - (P) (Leased equipment requirement)
438B. NONE - (P) (Leased equipment requirement)
440A. WILL NOT LEAK - CAT 6 - (P)
440B. WILL NOT LEAK - CAT 6 - (P)
444. INTERSTATE USE, 100 PERCENT - (P)
BT

If you require TSP line items 521, 525, 526A, B, and C, 529, and 531 are required. Refer to DISA Cir 310 130-1 page 3-58.

GLOSSARY:

SIPRNET-	**Secret Internet Protocol Router Network**
POC-	**Point Of Contact**
RFS-	**Request For Service**
TSR-	**Telecommunications Service Request**
TSO-	**Telecommunications Service Order**
TCO	**Telecommunications Certification Office**
CSU/DSU	**Channel Service Unit/Digital Service Unit ie: modem**
FE	**Field Engineer**
DOD	**Department of Defense**
DSS	**Defense Security Service**
SIPRNIC	**Secret Internet Protocol Router Network Information Center**
GFE	**Government Furnished Equipment**
RCC	**Regional Control Center**
PLA	**Plain Language Address**
Premise Routers	**These are customer owned equipments not to be confused with Hub equipments which are actually part of the SIPRNET.**
Backside Connections	**Those connections to premise equipments. Not to actual SIPRNET Hub.**
PDC	**Program Designator Code - Funding code. This is between 4 and 6 characters and is how DISA is paid for connections to the SIPRNET.**
DEMARC	**This is that point where commercial vendors terminate their connections at a particular facility. A phone closet, DCO (Dial Central Office) etc.**
IATC	**Interim Approval To Connect**
IATO	**Interim Approval to Operate**
DAA	**Designated Approving Authority**

JOINT STAFF INFORMATION

INFORMATION PAPER

Subject: Access Policy for Allies on the Secret Internet Protocol Router Network (SIPRNET)

Purpose. To provide information on the access policy and process for connecting allies to the SIPRNET

Major Points

Access Policy

SIPRNET is a Secret, US-only network. However, connections to agencies of foreign governments are permissible through the use of approved security devices employed on each foreign connection to the SIPRNET. These security devices must be in US controlled spaces.

The 7 Nov 95 MCEB approved the access approval process for allies on the SIPRNET

Access Approval Process

The CINC, as the sponsoring activity for the foreign connection, must first request Joint Staff/J6 approval of the requirement in accordance with CJCSI 6211.02A.

Joint Staff/J6 validates the requirement and forwards the request to DISA/NS522 (Network Services, Classified Network Branch) to work a technical solution.

The technical solution is worked jointly with the DISN Security Accreditation Working Group (DSAWG), DISA/NS522 CINC representatives. Additional technical expertise and assistance may be requested from NSA and the Joint Interoperability and Engineering Organization, as required.

After a technical solution has been decided, the solution is presented to the DSAWG for approval. If approved by the DISN Designated Approving Authorities (DAAs), which include the Joint Staff, DIA, NSA, and DISA, the DSAWG will advise both the sponsoring CINC and DISA/NS522 in writing.

The CINC coordinates with the SIPRNET project office in DISA/S522 to complete the SIPRNET connection.

J6 Point of Contact: **David Uhrich, Lt Col**
Joint Staff/J6T - 703-695-5898

The following has been extracted from an E-Mail sent by Joint Staff referring to Contractor Connections to the SIPRNET.

This e-mail contains information we send out to help SPONSORS prepare requests for SIPRNET connectivity for contractors. The DOD sponsor is responsible for submitting the SIPRNET access requests to Joint Staff/J6T. Once J6T has validated the requirement and OSD has approved it, the requests and approvals will go to DISA. The DISA customer rep is Jim Nostrant, (703) 735-3238. I understand it takes DISA approximately 90-120 days to provision your circuits after they receive your accreditation packages and our approvals. To assist you, I am enclosing three documents:

1. Example of a SIPRNET connection request letter (to be completed by the DOD sponsor). (See attach – SIPRxmpl.doc – 2 pages.) Items to include when drafting the letter include:

a) Needs to be addressed to Joint Staff/J6T
b) Identify the operational need for the requested connection
   * what work will the contractor be doing over this connection
   * what sites they need access to
   * what information and type of information will be passed over this connection
   * frequency this information will be passed (i.e. daily, weekly, monthly transmissions)
c) Identify government sponsor POC to include name, telephone and fax numbers
d) Identify contractor POC to include name, telephone and fax numbers
e) Identify duration of need for connection (if different than contract expiration date)
f) Identify the contract number and duration of the contract

Please do not fall into the trap of describing the importance of your project and/or all the things the contractor must do for your project. Rather, focus on why the contractor needs SIPRNET access to do those things. Please keep it unclassified, if at all possible.

2. CJCSI 6211.02A (see Enclosure A, paragraph 6d, in particular of attach -- 6211-02A.doc -- 24 pages.) Keep in mind that the DOD sponsor is responsible for paying for the contractor's connection to SIPRNET. If you have questions, please contact Mr Nostrant at DISA (identified above) about these costs.

3. DISA message 121713Z DEC 95 on SIPRNET interim connection requirements (see paragraph 2, in particular). (See attach -- DISAmsg.doc -- 3 pages.) The Defense Security Service (formerly known as the Defense Investigative Service) is responsible for accrediting the contractor facility and automated information system prior to connection to the SIPRNET. I suggest you or the contractor begin working on your accreditation package right away, because it usually takes a good deal of time to collect all the information and DISA will not start working your request until they receive both our approval and your accreditation package.

Some additional background: SIPRNET is DOD's primary command and control network. Contractors are only

allowed access when it is in the best interest of the DOD and implemented in such a way as to ensure the risk to the rest of the SIPRNET community is within acceptable levels. As the accreditors of the SIPRNET, these risk levels are established by the DISN Security Accreditation Working Group (DSAWG). The DSAWG has established the policy that contractor facilities can only be connected frontside to SIPRNET through a DISA controlled router. With the assistance of the sponsor, DISA will establish filters within the router to allow the contractors to access only those sites they need to fulfill their contractual responsibilities with the DOD. Granted, this may be a more expensive solution than having the contractor site connected through a backside router, but the need for security and control within the SIPRNET is of paramount importance.

You should contact Mr James Jones (703) 325-3917 or Mr Larry Moore at (703) 325-9495 for information on the release forms for each IP address your contractors will need connectivity with.

I hope this information helps. Please call me at DSN 227-7091, commercial (703) 697-7091 if I can be of any further assistance. Your request, preferably signed by an O-6 or equivalent with funds releasing authority, can be faxed to (703) 614-9364 to expedite processing. Request you follow-up by mailing the signed request to:

The Joint Staff, J6T
The Pentagon,
LTC David Uhrich
Washington, DC 20318-6000

Regards,

<<SIPRxmpl.doc>> <<DISAmsg.doc>> <<6211-02A.doc>>

EXAMPLE ONLY

Defense Threat Reduction Agency
45045 Aviation Drive
Dulles, VA 20166-7517

EXAMPLE ONLY

1 Sep 00

FROM: DOD ORGANIZATION X

MEMORANDUM FOR: Joint Staff/J6T (Attn: Lt Col Theresa Giorlando, Rm 1D826)

SUBJECT: Secret Internet Protocol Network (SIPRNET) Connectivity for United Research Associates (URA)

1. BACKGROUND: The DOD ORG X has developed a tool to aid the weaponeer in defeating high value targets containing weapons of mass destruction. The tool, called TEST X, was developed to fill a need arising from the Gulf War. It is fast-running and capable of running on a portable, relatively low-end machine. Our customer base has grown to nearly 300 users world-wide since the product's first release three years ago. We recently awarded a four-year contract to United Research Associates (URA) for further development of IMEA. This year we will be installing a web page on the SIPRNET to allow users to post problem reports, communicate with the developer, and obtain other information to facilitate warfighter use. URA has been tasked to trouble-shoot and resolve user problems on a real-time basis, and, if needed, to operate 24 hours per day in a help-desk mode. It is, therefore, essential that URA have access to the SIPRNET. Therefore, I request that URA be given access to the SIPRNET at their office in Raleigh, NC, for the purpose of supporting this program.

2. DISCUSSION:

a. Secure Development with Prime Contractor – There will be times when the weaponeer will need assistance in developing a weaponeering solution with TEST X. In crisis planning especially, quick resolution of problems will be critical. In order to assist the user in a timely manner, we may ask them to send us their work via the SIPRNET for analysis. URA, working with us, will provide advice to the user. If the problem resides in the programming code, URA will develop a fix and distribute that via the SIPRNET.

b. Exercise Support – DOD ORG X routinely supports CINC exercises throughout the world. As in crisis planning, there may be problems encountered while trying to weaponeer a target. Problems may involve techniques to model complex targets or developing unique work-arounds to compensate for unusual situations. URA is best suited to provide the modeling support, to analyze programming problems, and to develop fixes.

3. CONCLUSION: Approval of this request will provide for an efficient and economical way for DTRA to support the warfighter in crisis and deliberate planning missions as well as provide for an efficient method to release and update future versions of TEST X. URA, under contract DSWA01-98-C-0180, will require access to the SIPRNET through contract expiration on 31 Dec 01. Point of contact at URA is Mr. Robert Bean (alternate is Dr Frank Stein), phone (123) 456-7890; fax is (123) 456-4433. Point of contact at DOD ORG X is MAJ Steve Sponsor, DSN 555-1234, or commercial (123) 555-1234, fax (123) 555-0001.

LEON R. BOSS, Col, USMC
Program Manager, Special Weapons Targeting

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6

CJCSI 6211.02A
DISTRIBUTION: A, B, C, J, S 22 May 1996

DEFENSE INFORMATION SYSTEM NETWORK
AND CONNECTED SYSTEMS

References: See Enclosure C.

1. Purpose. This instruction establishes policy and delineates responsibilities for life-cycle management of the Defense Information
System Network (DISN). It details policy for management and use of the DISN, DISN services, and connected systems. Specific policies governing the satellite component of the DISN are covered in CJCS MOP 37, "Military Satellite Communications Systems."

2. Cancellation. CJCSI 6211.02, 23 June 1993, “Defense Information System Network and Connected Systems, is cancelled.

3. Applicability. This instruction applies to the Joint Staff, Services, CINCs, and Defense agencies.

4. Policy. The DISN is DOD’s consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. All DOD activities requiring telecommunications services will use the DISN when those services are available and are technically and economically feasible to the Department of Defense. See Enclosure A for general guidance on DISN management and use.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Procedures. This instruction provides policy guidance and, where
required, tasks the appropriate agencies to develop and publish detailed procedures.

8. Summary of Changes. This instruction establishes the DISN as the primary DOD end-to-end telecommunications network for supporting military operations. Subparagraph 6.e, of Enclosure A incorporates language from Change 2 of the Joint Ethics Regulation, DOD 5500.7, regarding the use of the DISN for health, morale, and welfare telephone calls and other authorized uses. This paragraph, as changed, also will change subparagraph 10a of Enclosure A of CJCSI 6215.01, 1 February 1996 to be

in agreement with DOD 5500.7

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

Enclosures:
A--General Guidance
Appendix--Guidelines for the DISN Requirements Committee
B--Organizational Responsibilities
C--References
GL--Glossary

DISTRIBUTION

Copies

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

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)..... 4

Director, National Security Agency/Chief, Central Security Service..... 4

Director, Joint Interoperability Test Center..... 2

Director, Inter-American Defense Board..... 2

Chairman, US Section US-Canada Military Cooperation Committee..... 2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

GENERAL GUIDANCE

1. System Concept

a. The DISN is DOD's worldwide protected network that allows the warfighter to exchange information in a seamless, interoperable, and global battlespace. Its underlying infrastructure is composed of three major segments or blocks:

(1) The sustaining base (i.e., base, post, camp, or station) C4I infrastructure (to include legacy systems) that will interface with the long-haul network in order to support the deployed warfighter (reach-back services).

(2) The long-haul telecommunications infrastructure, which includes the Defense Communications System (DCS) and the communication systems and services between the fixed environment and the deployed joint task force (JTF) and combined task force (CTF) warfighter.

(3) The deployed warfighter and associated commander in chief (CINC) telecommunications infrastructures that support the JTF and/or CTF.

b. The DISN long-haul infrastructure is an integrated network, centrally managed and configured to provide intersite and interelement/block information transfer services for all DOD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, and video services in support of national defense C4I decision support requirements and corporate information management (CIM) functional business areas.

c. The DISN provides the global transfer infrastructure by integrating separate CINC, Service, and Defense agency networking requirements into a DOD enterprise-wide network to meet common-user and special purpose information transfer requirements.

d. DISN information transfer facilities will support secure transmission requirements for subnetworks such as the Global Command and Control System (GCCS), Defense Red Switch Network, the Joint Worldwide Intelligence Communications System, and the Defense Message System (DMS).

2. Required Features. DISN will:

a. Be global in scope.

b. Be interoperable between all infrastructure segments or blocks.

c. Support multiple information transfer services for DOD users, including (1) dedicated point-to-point; (2) switched
voice and data, currently Unclassified but Sensitive IP Router Network (NIPRNET), and Secret IP Router Network (SIPRNET); and (3) video services.

d. Be capable of rapid expansion or reconfiguration (minutes and hours) and extension to the tactical environment, and be interoperable with tactical systems. Bandwidth capacity for surge will be engineered and

allocated based on contingency requirements and Joint Staff validation and direction.

e. Support automatic rerouting and restoral of circuits by priority in accordance with existing National Security-
Emergency Preparedness (NSEP) procedures, Telecommunications Service Priority (TSP) procedures, and other procedures as required to ensure network performance and user requirements are met.

f. Be operated, maintained, and managed under the full control of military and DOD civilian personnel.

g. Be robust, adaptive, and reliable by employing network and configuration management, diverse routing, and automatic rerouting features.

h. Provide subnetwork and component survivability commensurate with the supported command or mission.

i. Support multilevel precedence and preemption (to meet assured connectivity requirements) and all classifications of information.

j. Support value-added services, such as messaging and conferencing, and allow for the addition of new services and technologies.

k. Provide a secure information environment for the processing, storage, transfer, and use of information in accordance with the DISN security policy.

l. Be capable of detecting attempts to access the network by unauthorized users. Support automatic denial of such access attempts and automated reporting of such attempts to the DISN management structure.

3. Use. In accordance with procedures outlined in reference b, all DOD long-haul communications requirements will be submitted to DISA. DISA will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements. Sustaining base and deployable requirements will be processed in accordance with reference b and the supporting components' procedures.

4. Connection Requirements Identification. Each DOD system or application device having a requirement for long-haul common-
user information transfer services will be identified to DISA for DISN planning purposes. DOD activities will identify these systems and requirements to DISA as soon as requirements for these services have been validated.

5. Access and Connection Approval. The Chairman of the Joint Chiefs of Staff, Chiefs of the Services, CINCs, directors of Defense agencies, or their designated representative will validate operational requirements before requesting connection approval from DISA. Requirement validation and approval should ensure mission requirements are best satisfied via the DISN. DISA will make final approval for all DISN connections ensuring operational requirements have been validated; connections meet all technical and interoperability requirements; and subnetworks, systems, and other connected components provide adequate security and have been accredited by the proper authority. Requirement conflicts will be resolved by the DISN Requirements Committee or similar forum using guidelines in the Appendix.

6. Specific Provisions for Access and Connection

a. DOD Activities. DISA, in conjunction with the Services and agencies, will develop, coordinate, and publish DISN connection criteria and approve new connections for all DISN services for all activities.

b. Non-DOD Federal, State, and Local Government Activities. Requirements of non-DOD Federal, State, and local government activities will be submitted to the Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, for validation and then forwarded for OSD approval.

c. Foreign Governments and Allied Organizations. In addition to first meeting the access and connection requirements for non-DOD US activities, use of the DISN by foreign governments and allied organizations must be approved under the provisions of reference c.

d. Civilian Contractor Activities. Requirements for access of contractor-controlled systems to DISN must be validated by the Joint Staff and approved by OSD. Based on a US Government contract, authorized contractor personnel may use DOD-controlled systems with access to DISN when performing contractual responsibilities. The sponsoring agency validates and arranges funding for the requirement.

e. Health, Morale, and Welfare (HMW). DISN shall be for official use and authorized purposes only.

(1) Official use includes emergency communications and any other communications that the CINC determines are necessary in the interest of DOD. In the interest of morale and welfare, CINCs may approve communications by DOD employees and military members to their family members at home from locations to which they are deployed for extended periods of time on official business.

(2) Authorized purposes include, for example, brief communications made by military members and DOD employees during official travel to notify family members of transportation or schedule changes. Reasonable personal communications (such as auto or home repair appointments or brief Internet searches) from the military member or DOD employee at his or her workplace are also authorized when the CINC or Agency Designee permits categories of such communication and after determining that such communications:

(a) Do not adversely affect the performance of the DOD organization or the official duties of the military member or DOD employee.

(b) Are of reasonable duration and frequency, and whenever possible, made during the employee's or military member's personal time such as after normal duty hours or during lunch periods.

(c) Serve a legitimate public interest, such as enabling DOD employees or military members to stay at their desks rather than requiring them to depart the work area to use commercial systems, or improving the morale of military members and DOD employees stationed away from home for extended periods of time.

(d) Would not reflect adversely on DOD, such as uses involving pornography, chain letters, unofficial advertising or soliciting, inappropriate handling of classified information, etc.

(e) Do not overburden the communication system, create no significant additional cost to DOD, and in the case of long distance communications are:

1. Charged to the DOD employee's home telephone number or other non-Federal Government number (third number call).

2. Made to a toll-free number.

3. Reversed to the called party if a non-Federal

Government number (collect call).

4. Charged to a personal telephone credit card.

5. Otherwise reimbursed to DOD or the DOD component in accordance with established collection procedures.

7. Security. DISN will support and employ security services, protection mechanisms, and procedures in accordance with referenced and subsequent revisions of the DISN security policy. The DISN Security Accreditation Working Group will provide, interpret, and approve DISN security policy and, under Defense Information System Security Program (DISSP) sponsorship, will make accreditation recommendations to the four designated approval authorities (DAAs) (the Directors of DISA; NSA/Chief, CSS; DIA; and the Joint Staff) for the DISN.

a. Connected systems will be secured commensurate with the sensitivity of the information (both classified and unclassified) being processed.

b. Users must comply with DOD security requirements as described in references e and f for those systems processing Sensitive Compartmented Information (SCI) and implementing Service and Defense agency directives.

c. Connection to any other automated information system or data communication network or subnetwork, while connected to DISN, is strictly prohibited without appropriate documentation from the DAAs of the connected networks.

d. Security requirements for DISN elements and connected systems accessing DISN will be contained in reference d, subsequent revisions, and guidance provided by DISA's Center for Information System Security (CISS).

8. Cost Recovery. In accordance with OSD direction, DISN non-Defense Satellite Communication System costs will be recovered through the Defense Business Operating Fund (DBOF) Communication Information Services Activity (CISA) through a billing scheme that is published by DISA. Non-DOD activities will be billed through the respective Service or Defense agency approval authority.

9. New DISN Services. DISA will continually assess the technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN. The CINCs, Services, and agencies will provide similar assessments regarding the sustaining base and deployable infrastructure. New services and capabilities will be added in response to validated user requirements and via planned technology insertion.

10. Survivability. Survivability enhancements in transmission paths, routing, equipment, and associated facilities will normally be limited to systems supporting units with critical missions that justify the additional cost.

APPENDIX TO ENCLOSURE A

GUIDELINES FOR THE DEFENSE INFORMATION SYSTEM
NETWORK REQUIREMENTS COMMITTEE

1. Purpose. To provide a forum for resolution of requirement issues for the DISN.

2. Representation. The committee will consist of representatives of the Joint Staff, Services, Defense agencies, unified commands, and DISA. The Director, J-6, will appoint the committee chair.

a. Representatives should be O-6 or civilian equivalent.

b. CINCs will participate but may arrange to delegate their issues to the Joint Staff for resolution. Services and Defense agencies should coordinate issues with the supported CINC.

c. All representatives are expected to present the staffed viewpoint of their parent organization.

3. Meetings. The committee will meet as required to resolve unsettled DISN requirements issues.

4. Resolution Process. Unresolved issues will be forwarded to the Military Communications-Electronics Board (MCEB) for resolution through the MCEB process.

(INTENTIONALLY BLANK)

ENCLOSURE B

ORGANIZATIONAL RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff is responsible for operational network policy and overall direction. The Director, Joint Staff, serves as one of the four DAAs for DISN accreditation issues. Authority for operational DISN policy and direction is delegated to the Director, J-6, Joint Staff, who will:

a. Monitor the operational and management effectiveness of the network and report significant items (e.g., major mission degradation) to the Chairman of the Joint Chiefs of Staff.

b. Use the requirements committee and the MCEB to resolve requirements conflicts and issues referred to the Joint Staff. Guidelines for the requirements committee are delineated in the Appendix to Enclosure A.

c. Coordinate and assign funding responsibility for joint requirements to the appropriate Service.

d. Validate unified command, Service, or Defense agency subnetworks.

e. Validate non-DOD Federal, State, and local government requirements.

2. The CINCs will:

a. Define, validate, and coordinate DISN candidate information system requirements.

b. Review and submit service restoration priority requests in accordance with NSEP and TSP procedures.

c. Delegate validation authority, as deemed appropriate, to supporting Services and Defense agencies.

d. Ensure approved systems efficiently use DISN services to meet mission requirements and enforce user compliance with DISN policy and procedures.

e. With the exception of USCINCSOC, submit their validated DISN requirements through Service channels to DISA. USCINCSOC will submit service requirements directly to OSD.

3. The Director, DISA, is assigned overall responsibility as DISN network manager and, in accordance with reference g, will:

a. Provide operational management for the DISN and will be responsive to the validated operational requirements of the Joint Staff, CINCs, Services, and Defense agencies.

b. Establish a management structure for DISN and exercise operational direction, including day-to-day network management and configuration management of the DISN (i.e., maintaining an accurate and appropriately classified data base of existing DISN users, including non-DOD activities, and monitoring system service restoral to ensure compliance with NSEP and TSP procedures).

c. Perform required system engineering and modeling to achieve optimal network design and implementation approach, and identify performance standards for DISN services (i.e., availability and response time).

d. Continuously monitor the effectiveness of the DISN and provided services in satisfying user requirements. Be responsive to CINC requests for reports on system performance.

e. Refer to the Joint Staff any matters that significantly degrade the network.

f. Provide Joint Staff, Services, Defense agencies, and CINCs appropriate periodic status and programmatic

updates.

g. In coordination with the Joint Staff, and the appropriate CINCs, Services, and Defense agencies, analyze and satisfy requests for new DISN services.

h. Specify interoperable interface protocol standards, in coordination with the CINCs, Services, and Defense agencies.

i. Coordinate changes, through the requirements committee, that impact user interfaces.

j. Establish and publish DISN connection requirements identification and accreditation procedures and publish to the unified commands, Services, and Defense agencies.

k. Develop and maintain a coordinated Test and Evaluation Master Plan and provide operational test and evaluation through the Joint Interoperability Test Center to ensure user network requirements are being met. Additionally, DISA will chair periodic working groups with Service and DOD agency representatives on all DISN-related network level acquisitions and changes.

l. Ensure that the DISN security architecture meets the needs of DISN users.

m. Develop and maintain DISN planning and program management process and documentation.

n. Ensure security measures and plans and accreditation policies are based on threat assessments validated by the appropriate member(s) of the DOD Intelligence Community.

o. Serve as one of the four DAAs for the DISN.

4. The Services and Defense agencies will:

a. Review long-haul common-user transmission requirements and forward all requirements not needing unified and specified command, Joint Staff, or OSD approval to DISA for development of a technical solution, coordination, and implementation. In accordance with DISA provided criteria, systems requirements must be identified far enough in advance to ensure a timely acquisition of network components to satisfy the required operational date.

b. Review and submit, as delegated by the supported CINC, requirements for service restoral capability with sufficient information as prescribed in reference h.

c. Program, budget, fund, and provide support for assigned portions of the DISN through the PPBS, including approved contractor and foreign government systems.

d. Provide sufficient local data distribution capability to meet the CINC's validated connectivity requirements. (These systems must be focused on supporting operational requirements of the parent Service and be capable of supporting a joint task force headquarters to support contingencies.)

e. Apply applicable information, communications, and physical security measures and ensure installation requirements continue to meet the requirements of the DISN security policy.

f. Ensure that approved systems use DISN services to meet mission requirements and ensure user compliance with DISN policy and procedures.

g. Coordinate with the theater commander and DISA before submitting long-range requirements for DISN access within a geographic region of responsibility of a theater unified command. Conflicting views among the requesting activity, DISA, and the concerned commander of a unified command will be forwarded to the J-6, Joint Staff, for resolution.

h. Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits according to DISA-established criteria. Services and DOD agencies will provide representatives to joint, DISA-chaired working groups on related topics.

i. Provide requisite site support for the DISN equipment located on their respective bases, posts, camps, and stations. Site support requirements will be specified by DISA in appropriate procedural documentation and coordinated with the Services and Defense agencies. Support required will include, but is not limited to, providing power, physical security, floor space, and on-site coordination for the DISN data networks points of presence located on their respective bases, posts, camps, and stations.

j. Manage DISN subnetworks when authorized by the Director, J-6, Joint Staff.

k. Provide information, as requested, to DISA for DISN billing, management, and inventory purposes.

l. Identify representatives to the DISN Requirements Committee and its subcommittees, as required.

m. Implement and comply with the policies and procedures required in references a and b.

5. The Director, NSA/Chief, CSS, will:

a. Provide guidance on required security services and features necessary to meet DISN operational requirements.

b. Recommend basic doctrine, methods, and procedures to minimize DISN information security vulnerabilities in accordance with the provisions of references i and e.

c. Validate all requirements for, manage, and accredit all NSA/CSS cryptologic systems in accordance with references e and f.

d. Serve as one of the four DAAs for the DISN.

e. Develop, acquire, and certify COMSEC equipment.

6. The Director, DIA, will:

a. In accordance with established agreements with DISA, implement, operate, and manage Joint Worldwide Intelligence Communications System (JWICS) components and facilities on the DISN.

b. Serve as one of the four DAAs for the DISN.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DODD 4640.13, 5 December 1991, "Management of Base and Long-Haul Telecommunications Equipment and Services" (currently under revision)

b. DODI 4640.14, 6 December 1991, "Base and Long-Haul Telecommunications Equipment and Services" (currently under revision)

c. CJCS MOP 43, 11 March 1992, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

d. DISN Long-Haul Security Policy, 14 December 1995

e. DODD 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems (AISs)"

f. DCID 1/16, 19 July 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks"

g. DODD 5105.19, 25 June 1991, "Defense Information Systems Agency"

h. DISA Circular 310-130-4, 18 August 1993, "Defense User's Guide to the Telecommunications Service Priority (TSP) System"

i. DODD C-5200.5, 21 April 1990, "Communications Security (COMSEC)"

j. DODD S-5100.19, 19 March 1959, "Implementation of National Security Council Intelligence Directive No. 7"

k. CJCS MOP 37, 14 May 1992, "Military Satellite Communications Systems"

(INTENTIONALLY BLANK)

GLOSSARY

application devices. Devices (e.g., computer terminals, personal computers, mini and mainframe computers, and facsimile machines) that provide a capability to process information from various input mechanisms.

data communications. Information exchanged between end systems in machine-readable form.

Defense Business Operations Fund (DBOF), Resource Management Committee. Committee which coordinates the funding of the DCS.

Defense Information System Network (DISN). A subelement of the Defense Information Infrastructure, the DISN is the DOD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Defense Satellite Communications System (DSCS). Composed of DOD operated and maintained satellites and earth terminals, operating in the SHF frequency band, that provide communications transmission capability.

Designated Approving Authority (DAA). Responsible for weighing the security risks of operating an automated information system versus the benefits it may provide and deciding whether or not to approve operation of the system.

DISN user. An individual assigned to an organization having devices directly or indirectly connected to the DISN.

Military Communications-Electronics Board. A decision making body chaired by the Joint Staff, J-6, and composed of the C4 heads of the Services, DIA, and NSA and the Director, DISA.
This body deals with issues of interoperability and standardization between the Department of Defense and US allies.

subnetwork. A logical partition of a network amenable to separate management, control, and provisioning because of functional or geographic reasons.

system. A generic term for a collection of equipment connected to the DISN. It may refer to a host, a group of hosts, or a network.

validation. The confirmation, by designated authority, that a request for access and use of the DISN is necessary to meet that organization's mission requirements.

Warner-Exempt. Guidelines used to determine if system acquisition must be conducted through GSA. As a general guideline, systems that directly or indirectly support a warfighting mission are considered Warner-Exempt and do not require acquisition through GSA.

U N C L A S S I F I E D

ROUTINE CHANNEL NO. 318992 04-22-96

RCTUZDKW RUEJDCA2712 1131812 MTMS-UUXX—XXXXXXX.1131822 318992 04-22-96
ZNR UUUXX
R 121713 DEC 95
FM DISA WASHINGTON DC//D343//
TO CONUSMILNETSTA
CONUSDSNET1STA
AIG 8787
AIG 8791
RUENAAA/CNO WASHINGTON DC//N6/N61/N62/N643//
RUEACMC/CMC WASHINGTON DC//C4I/CS/CCT//
RUEAHQA/HQ USAF WASHINGTON DC//SC/SCM/AQPC//
RUEADWD/DA WASHINGTON DC // DISC4/SAIS-ADM/DAMO-FD//
INFO RUEKJCS/SECDEF WASHINGTON DC//OASD:C3I//
RUEKJCS/JOINT STAFF WASHINGTON DC//J3/J6/J6S/J6T/J6V/J6Z//
RUEOFFA/ESC HANSCOM AFB MA//AVN//
RHCUABA/HQ AFC4A SCOTT AFB IL//XPR//
RUEANBA/PM AWIS FT BELVOIR VA//SFAE-CC-AWT//
RUFTDCA/DISA EUR VAIHINGEN GE//EU/EU2/EU21//
RUHHAAA/DISA PAC WHEELER AAF HI//PC/PC2/PCC//
RUEOBSA/DISA CENTRAL COMMAND FWD//JJJ//
RUCJICD/DISA CENTRAL COMMAND MACDILL AFB FL//DF//
RUEAHUA/CDRUSAISC FT HUACHUCA AZ//ASOP//
RUVOBTA/HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
RULSWCB/COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
RUETIAA/DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y441//
RUETICO/NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE MD//Q214//
RUET1AA/NSACSS FORT GEORGE G MEADE MD//Y443//
RUEOASI/ISPO ANNAPOLIS JUNCTION MD//JJJ//
RULSJGA/COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//
RULSJGA/COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
RUEADNA/DNA WASHINGTON DC//COMP-1/NOCC//
RUEANLA/DLA FT BELVOIR VA//CANAI//
RUDIDLJ/DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
RUEKJCS/JOINT STAFF WASHINGTON DC//J6T/J8//
RUCJACC/USCINCCENT MACDILL AFB FL//J6//
RUCJAAA/USSOCOM MACDILL AFB FL//J6//
RHHMUNA/USCINCPAC HONOLULU HI//J6//
RUCEAAA/HQ USSPACECOM CHEYENNE MOUNTAIN AS CO//J6//
RUCUSTR/USSTRATCOM OFFUTT AFB NE//J6//
RHCUAAA/USTRANSCOM SCOTT AFB IL//J6//
ACTION D322 ADDR BY: 31 INTERNALLY GENERATED DISTRIBUTION COPY
INFO D6-JE D331 D31 DO WEY WE34 D2 D23 JEE JEJ JEX D21 D3 D333 D8 ISB JEB
THIS MESSAGE IS A RETRANSMISSION
RUEJDCA 2712 121713Z DEC 95

UNCLASSIFIED

UNCLASSIFIED

RHLBAAA/HQ SOUTHCOM QUARRY HEIGHTS PM//J6//
RUCBACM/USACOM NORFOLK VA//J6//
RUSNNOA/USCINCEUR VAIHINGEN GE//J6//

RUEASRB/CDRFORSCOM FT MCPHERSON GA//AFIS-O//
RUDHDMH/HQ DMA FAIRFAX VA//TSCEID//
RUEKJCS/DMSSC WASHINGTON DC//EIT/TCO//
RHCUAAA/DITCO SCOTT AFB IL//DTS//
RUWTSGT/DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN
RHCUABA/DISA SCOTT AFB IL//UNR/UNRSE/UNRSO//
RUEKDIA/DIA WASHINGTON DC//SC/SY/SY-3A/SY-3C//
RULSGAE/NAVCOMTELSTA WASHINGTON DC//N912//
RUCTPOL/NAVCOMTELSTA PENSACOLA FL//N51/N32//
RUEBAFA/JSC ANNAPOLIS MD//INS//
RUEARNG/ARNGRC ARLINGTON VA//NGB-AIS-SC//
RHDJAAA/CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
RUDIZA/DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
RUDIDFE/DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB/DFAS-IN-MI//
RUERFCP/CDRUSAISC COROZAL PM//ASNP-OPS//
RUDIDSA/DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
RUWTNOK/DISA FLD OFC PETERSON AFB CO//JJJ//
RUEASRA/DISA FLD OFC FT MCPHERSON GA//SANM//
RUEOBSA/DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
RUCBSAA/DISA FLD OFC NORFOLK VA//FAN//
RHLBAAU/DISA FLD OFC QUARRY HEIGHTS PM//
RULSWCD/DISA DCO-NCR RESTON VA//JJJ//
RHCUABA/DISA DCO-SCOTT SCOTT AFB IL//DRC//
RUEAHUT/DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
RUEJDCA/DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC/D2/D21/D3/D34/D343/D381
/JE/JT/WE/WEZ51/WE312//
BT
UNCLAS
OPER/CONUSMILNETSTA 06/95/CONUSDSNET1STA 04/95/ZDK RETRANSMISSION
DUE TO NUMEROUS REQUESTS/REF DISA D343/182100Z APR 96//
SUBJ/DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)
INTERIM NETWORK CONNECTION REQUIREMENTS//
REF/A/DOC/CJCSI 6211.02, DEFENSE INFORMATION SYSTEM NETWORK AND
CONNECTED SYSTEMS, 23 JUN 93//
REF/B/DOC/CJCS MOP 43, MILITARY TELECOMMUNICATIONS AGREEMENTS AND
ARRANGEMENTS BETWEEN THE UNITED STATES AND REGIONAL
DEFENSE ORGANIZATIONS OR FRIENDLY FOREIGN NATIONS, 11 MAR 92//
POC/JOSEPH BOYD/GS/D34/LOC:DISA WASH/TEL:DSN 653-8290/TEL:COMM
(7030735-8290//
RMKS/1. IAW REFERENCE A, CHAIRMAN OF THE JOINT CHIEFS OF STAFF
INSTRUCTION, ENCLOSURE B, PARA. 3.J., DISA WILL "ESTABLISH AND
PUBLISH DISN CONNECTION REQUIREMENTS, IDENTIFICATION AND
ACCREDITATION PROCEDURES, AND PUBLISH TO THE UNITED AND SPECIFIED
COMMANDS, SERVICES, AND DEFENSE AGENCIES." DISA IS CURRENTLY IN THE
PROCESS OF WRITING THE CONNECTION REQUIREMENTS FOR THE DEFENSE

UNCLASSIFIED

INFORMATION INFRASTRUCTURE (DII). DISA IS COMMITTED TO ENSURING THE
PROTECTION OF THE DII AND PROVIDING INFORMATION SYSTEMS SERVICES TO
THE WARFIGHTER. THE PURPOSE OF THIS MESSAGE IS TO PROVIDE EXISTING
AND POTENTIAL SIPRNET SUBSCRIBERS WITH CONNECTION REQUIREMENTS
THAT MUST BE FOLLOWED UNTIL THE DII REQUIREMENTS ARE PROMULGATED
(ESTIMATED $2^{ND}/3^{RD}$ QTR FY96). THE DII CONNECTION REQUIREMENTS WILL

IDENTIFY SECURITY REQUIREMENTS AND PROHIBITIVE ACTIONS REGARDING SIPRNET NETWORK ACCESS.
2. THE FOLLOWING REQUIREMENTS MUST BE MET BEFORE A NEW CONNECTION TO THE SIPRNET IS GRANTED.

A. CONTACT SIPRNET PROJECT OFFICE: AL CONUS CUSTOMERS DESIRING A DIRECT CONNECTION TO THE SIPRNET MUST FIRST MAKE CONTACT WITH THE PROJECT OFFICE, DISA/D343. PLEASE CONTACT MR. JOSEPH BOYD (SIPRNET PROJECT MANAGER) AT (703) 735-8290 (DSN 653-8290) OR MR. JIM NOSTRANT AT (703) 735-3238. EUROPE CUSTOMERS ARE TO CONTACT MR. BOB MAULDIN, DISA-EUR, AT DSN 314-430-8457. PACIFIC CUSTOMERS ARE TO CONTACT MR. LESTER PANG, DISA-PAC, AT DSN 315-456-2858.

B. SYSTEM SECURITY PACKAGE: IN ORDER FOR DISA TO APPROVE CONNECTIVITY TO SIPRNET, ALL AUTOMATED INFORMATION SYSTEMS (ais) CURRENTLY CONNECTED OR DESIRING CONNECTIVITY MUST SUBMIT THE BELOW LISTED DOCUMENTATION TO THE DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D343 (JOSEPH BOYD), 11440 ISAAC NEWTON SQUARE, RESTON VA 22090-5087

- ACCREDITATION LETTER. SIGNED BY THE COGNIZANT DESIGNATED APPROVAL AUTHORITY (DAA) FOR THE NETWORK/SYSTEM REQUIRING SIPRNET CONNECTION. IF THE AIS IS NOT ACCREDITED, INDICATE IF SYSTEM IS OPERATING UNDER AN INTERIM APPROVAL TO OPERATE (IATO). THE SIPRNET CONNECTION WILL NOT BE GRANTED UNLESS EVIDENCE OF AN ACCREDITATION OR IATO IS PROVIDED.
- INTERIM APPROVAL TO OPERATE. IF AN IATO HAS BEEN GRANTED, ADVISE THIS OFFICE OF ALL SIGNIFICANT RISKS THE SYSTEM IS CURRENTLY OPERATING UNDER. SIGNIFICANT RISKS INCLUDE LACK OF IDENTIFICATION AND AUTHENTICATION MECHANISMS, LACK OF AUDIT FUNCTION, UNPROTECTED CONNECTIONS TO OTHER NETWORKS, UNAUTHENTICATED AND UNPROTECTED DIAL-IN CAPABILITIES, ETC.
- AIS CONCEPT OF OPERATIONS AND SECURITY POLICY OF EQUIVALENT DOCUMENTATION. THESE SECURITY DOCUMENTS WILL DESCRIBE HOW SECURITY REQUIREMENTS HAVE BEEN IMPLEMENTED IN THE ENVIRONMENT FURTHER, THESE DOCUMENTS WILL IDENTIFY DATA TYPES, CLASSIFICATION LEVEL OF DATA, SYSTEM OWNER, AND DESIGNATED APPROVING AUTHORITY.
- SYSTEM CONNECTIVITY DIAGRAM. THIS DIAGRAM SHALL IDENTIFY ALL AIS CONNECTIONS, BOTH FRONT AND BACKSIDE., TO INCLUDE ANY CONNECTIONS TO OTHER GATEWAYS DIRECTLY OR INDIRECTLY CONNECTED TO OTHER NETWORKS.
- FOREIGN CONNECTIONS. THE SIPRNET IS A "SECRET, SYSTEM HIGH, U.S. ONLY" NETWORK. HOWEVER, CONNECTIONS TO AGENCIES OF

UNCLASSIFIED

FOREIGN GOVERNMENTS MAY EXIST. ALL FOREIGN CONNECTIONS TO THE SIPRNET MUST FIRST BE VALIDATED BY THE JOINT STAFF (UNDER THE PROVISIONS OF REF B) AND APPROVED IN ACCORDANCE WITH THIS MESSAGE. ALL FOREIGN CONNECTIONS WILL REQUIRE THE INSTALLATION OS A HIGH ASSURANCE GUARD DEVICE OR AN END-TO-END ENCRYPTION DEVICE. BOTH TYPES OF DEVICES SHALL BE UNDER US CONTROL (PROCURED, OPERATED,

MAINTAINED, AND CONFIGURED BY THE U.S. SPONSORING ACTIVITY) AND UTILIZED TO PREVENT UNAUTHORIZED OR ACCIDENTAL DISCLOSURE OF CLASSIFIED, U.S. ONLY INFORMATION ON THE SIPRNET.

- ACKNOWLEDGMENT OF PERIODIC MONITORING AND VULNERABILITY ASSESSMENTS. ALL CONNECTION REQUESTS MUST PROVIDE THE FOLLOWING STATEMENT: "WE ACKNOWLEDGE AND CONSENT TO DISA CONDUCTING AN INITIAL VULNERABILITY ASSESSMENT AND PERIODIC UNANNOUNCED VULNERABILITY ASSESSMENTS ON THE CONNECTED HOST SYSTEMS TO DETERMINE THE SECURITY FEATURES IN PLACE TO PROTECT AGAINST UNAUTHORIZED ACCESS OR ATTACK."

3. THE FOLLOWING REQUIREMENTS MUST BE MET FOR EXISTING SIPRNET CONNECTIONS. THE REQUIREMENTS IDENTIFIED IN PARA 2 APPLY. AN INTERIM APPROVAL TO CONNECT TO SIPRNET IS GRANTED FOR 90 DAYS FROM THE DTG OF THIS MESSAGE. WITHIN THIS TIMEFRAME, THE COGNIZANT SERVICE/ AGENCY MUST SUBMIT THE SYSTEM SECURITY PACKAGE WITHIN 90 DAYS OF THE DTG OF THIS MESSAGE. FOREIGN CONNECTIONS MUST BE IDENTIFIED, VALIDATED, AND APPROVED BY THE JOINT STAFF DURING THIS TIMEFRAME. FAILURE TO COMPLY MAY RESULT IN SERVICE DISRUPTION.

4. DISA RESERVES THE RIGHT TO DENY OR DISCONTINUE SIPRNET ACCESS TO RISK
ANY NETWORK OR SYSTEM DEMONSTRATING BEHAVIOR THAT INCREASES TO THE SIPRNET INFRASTRUCTURE AND TO SIPRNET SUBSCRIBERS.

5. THE DISN CERTIFICATION AUTHORITY (DISA CISS) WILL REVIEW THE ABOVE REQUESTED DOCUMENTATION AND MAKE A CONNECTION APPROVAL DETERMINATION. THE JOINT STAFF WILL VALIDATE AND APPROVE ALL FOREIGN CONNECTIONS. UPON REVIEW OF THE DOCUMENTATION PROVIDED AND INITIAL SECURITY CONCERNS ARE SATISFIED, THE CISS WILL ISSUE AN INTERIM APPROVAL TO CONNECT TO THE SIPRNET FOR A PERIOD OF 90 DAYS. THE FINAL APPROVAL TO CONNECT WILL BE PROVIDED BASED ON SUCCESSFUL COMPLETION OF THE VULNERABILITY ASSESSMENT AND SATISFACTION OF SECURITY DOCUMENTATION. SIPRNET REQUESTS FOR SERVICE AND FEEDER TSR'S CAN BE SUBMITTED CONCURRENT WITH THE ABOVE DOCUMENTATION; HOWEVER, CONNECTION ACTIVATION WILL NOT OCCUR UNTIL AN INTERIM CONNECTION APPROVAL IS GRANTED IN WRITING.

6. REQUEST DISA-EUROPE AND DISA-PACIFIC PROVIDE FURTHER DISSEMINATION OF THIS MESSAGE WITHIN YOUR RESPECTIVE THEATERS.

7. DISA POC IS MR JOSEPH BOYD, DSN 653-8290/COMM 703-735-8290.//

BT

Note** Item #7 changed to Mr John Staples (DSN) 653-3236 (Comm) 703-735-323

UNCLASSIFIED

SECURITY PACKAGE INFORMATION

1. **Customer is required to complete the Security Accreditation documentation and return to NS52. They must also understand that this is parallel with other efforts to be completed for connectivity. The specific POC within NS52 for security package information is as follows:**

Any questions regarding Security Packages and their requirements should be addressed to:
Mr. John Staples 703-882-2116, (DSN: 381) STAPLESJ@NCR.DISA.MIL

Mailing Address for Security Accreditation Package:

John Staples
Defense Information Systems Agency (NS 521)
5275 Leesburg Pike (1N031F)
Falls Church, Virginia. 22041

A. Package will consist of the following as the Security Checklist for Interim Approval to connect to the SIPRNET.

1. Evidence of Risk Acceptance by cognizant authority.

a. An Accreditation letter or Interim Approval to Operate (IATO) signed by the DAA.

1. This letter should state the following:

a. The System

b. Mode of Operation
1. System High
2. Dedicated
3. Multi Level
4. Periods Processing

c. Maximum level of sensitivity of information processed.
1. Unclassified (U)
2. Sensitive but Unclassified (N)
3. Confidential (C)
4. Secret (S)
5. Top Secret (TS)

d. Statement of the Residual/Significant Risk assumed by the DAA.

1. This is a summary of the results of a risk assessment.
2. This to include risks presented by connected networks/ systems

2. Statement of Minimum Security Requirements

a. Security Policy
b. System Security Plan

3. Statement of Specific Security Features and Implementation.

a. Concept of Operations
b. Security Concept of Operations

c. Security Standard Operating Procedures

4. System Connectivity Drawing/Configuration/Topology

a. Indicate connection to SIPRNET
b. Show connections to other networks/systems
c. Show proposed connections to other networks/systems

5. Provide MOAs/MOUs/Letters of Agreement of all connections to other networks/ systems.

a. Identify connections to NON-DOD networks/systems

6. Consent to DISA Monitoring statement per DISA message DTG 121713 DEC 95. Subject DISN SIPRNET Interim Network Connection Requirements.

7. System Identification

a. IP Address of premise router
b. List Authorized, (SIPRNET REGISTERED), Class B and Class C licenses

8. Security Checklist / SIPRNET Access Assessment – See forms further in document.

CONTRACTOR FACILITY CONNECTIONS / SECURITY PROCESS

A. Contractor facility connections vary somewhat from those connections for DOD Service or Agencies.

1. **Sponsor contacts J6 for validation of requirement.**

2. **J6 sends approval to NS52 / Mr. John Staples**

3. **NS52 sends copy of approval to DSS / Mr. Jim Jones along with name and number of customer and sponsor.**

4. **DSS contacts customer and DSS Field Office for action/IATO. Field Office involved determined by geographical location of customer requirement.**

    a. **Security Package submitted by DSS (Field Office) based on information received from customer.**

    b. **IP Addresses determined by DSS Field Representative and sent to Mr. Larry Moore at DSS Headquarters.**

5. **Full Security package sent from DSS to DISA, NS521.**

6. **DISA, NS521 issues Interim Approval TO Connect (IATC).**

7. **Customer Connects to SIPRNET.**

Checklist for SIPRNet Connection

Package #_____ CCSD#_____

The following 7 items are mandatory requirements to obtain the Interim Approval to Connect (IATC).

1. Evidence of Risk Acceptance by cognizant authority (Submit one of the following):

___ Approval to Operate (ATO)/Accreditation signed by Designated Approving Authority (DAA) - Valid for up to three years (the mode of operations and level of sensitivity of information being processed must be included).
Expiration:_____

___ Interim Approval to Operate (IATO) signed by DAA (Valid for up to one year)
(If submitting an IATO, the Statement of Residual/Significant Risk, Mode of Operations and Maximum level of sensitivity of information being processed must be included)
Expiration:_____

2. Mode of Operations: ____System High
____Dedicated
____Multi Level

3. Maximum level of sensitivity of information being processed:
   ____Unclassified
   ____Sensitive but Unclassified
   ____Confidential
   ____Secret
   ____Top Secret

4. System Connectivity Drawing/Configuration/Topology
   (to include hubs, bridges, routers, guards, firewalls, major applications (i.e. – GCCS, CIS, DMS), gateways, modems, card readers, backup devices, room and bldg. number, surge protectors, UPS, and A-B switches, backside connections, IP addresses, encryption devices)

5. Consent to Monitoring Statement signed by DAA

6. SIPRNet Access Assessment (SAA) Date:_____
   ___Yes: 1 2 3 4 5 6 7 8 (circle applicable numbers) ___All No

7. Joint Staff Approval: Yes_____ No_____ Not Applicable _____
   (Mandatory for Contractor, Foreign Connections, Non DoD Agencies, Exercises)
   POC is Joint Staff (J6T) at COMM 703-695-5898 (DSN: 225)

The following 5 items are mandatory requirements to obtain a final Approval to Connect (ATC).

1. If an ATO was not submitted in initial accreditation package then an ATO is required for ATC (the mode of operations and level of sensitivity of information being processed must be included).

2. Statement of Minimum Security Requirements as referenced in your CINCs/Services/ Agency's) System Security Instruction/Directive (must have at least one):
   ____Security Policy ____Security Directive
   ____Security Instruction ____Other (specify)_____

3. A Copy of Site Specific Security Features and Implementations (must have at least one):
   ____SSAA ____Security CONOP
   ____Security SOP ____Other (specify)_____

4. Copies of any other external connections and/or associated operational agreements (must have at least one):
   ____MOAs/MOUs ____Letters of Agreement
   ____Not Applicable Statement

5. IP Registration:_____ ____Yes ____No
   (To register the IP address contact the SIPRNet Support Center at 800-582-2567)

6. Completion of the compliance assessment by the DISA SIPRNet CAP Team (NS521)

Interim Approval to Operate (IATO) Letter Requirements

The IATO grants temporary authorization to process information under defined conditions. The letter will contain:

- The organization's letterhead and date of signature
- The specified security mode of operations and a specified data sensitivity or classification level
- Defined security safeguards (i.e., administrative, physical, personnel, COMSEC, emission, and computer security controls)
- System/Operational Applications (GCCS, DMS, CIS etc)
- A defined threat and stated vulnerabilities
- Stated interconnection to other systems
- A statement of acceptance of risk for the system
- A specified period of time (Up to one year maximum)
- A specified suite of hardware and software
- A specified operational environment
- Signature and signature block of the DAA

Sample IATO Letter

CINCs/Services/Agency's Letterhead
Address

Date

SUBJECT: Interim Approval to Operate (IATO) the Secret Internet Protocol Router Network (SIPRNet) for CCSD: _____

Ref: (a) Accreditation Support Documentation

1. In accordance with the provisions of ***(CINCs/Services/Agency's)*** Instruction ***xxxx***, an Interim Approval to Operate (IATO) is hereby granted to the ***(CINCs/Services/Agency's)*** Network, located in building ***xxxx,*** room ***xxxx, to include (list major applications), address***. This IATO is based upon a review of the information provided in reference (a). This IATO is valid for as long as the Baseline Security safeguards defined in the ***(CINCs/Services/Agency's specific security directives and guidelines)*** are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the ***(CINCs/Services/Agency's Baseline Security Documents)***. The IATO system consists of ***(equipment list)***. This system is authorized to ***process (place maximum level of information being processed) in the (mode of operation).*** The ***(CINCs/Services/Agency's)*** network is connected to SIPRNet and ***(place any other network that may be connected)***.

2. This IATO is valid for ***up to one year*** from the date of this letter. Final accreditation action is required before the expiration date of this IATO. This IATO will terminate sooner if there are any changes that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this IATO.

4. The undersigned accepts the risk for the operation of the ***(CINCs/Services/Agency's)*** system defined above.

Signature

Designated Approving Authority
CINCs/Services/Agency's

Sample IATO Letter When Submitting Supplemental Information that Changes Configuration

CINCs/Services/Agency's Letterhead
Address

Date

SUBJECT: Interim Approval to Operate (IATO) due to the ***(write reason – exercise, addition, deletion etc)*** the Secret Internet Protocol Router Network (SIPRNet) for CCSD: _____

Ref: (a) Accreditation Support Documentation

1. In accordance with the provisions of ***(CINCs/Services/Agency's)*** Instruction ***xxxx***, an Interim Approval to Operate (IATO) is hereby granted to the ***(CINCs/Services/Agency's)*** Network, located in building ***xxxx***, room ***xxxx, address (This should be what your current IATC/ATC reflects)***. This IATO is based upon a review of the information provided in reference (a). This IATO is valid for as long as the Baseline Security safeguards defined in the ***(CINCs/Services/Agency's specific security directives and guidelines)*** are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the ***(CINCs/Services/Agency's Baseline Security Documents)***. The IATO system consists of ***(equipment list). (Address what the reason you are submitting the updated DAA letter if due to major configuration change – include rooms, bldgs., applications, etc).*** This system is authorized to process ***(place maximum level of information being processed) in the (mode of operation).*** The ***(CINCs/Services/Agency's)*** network is connected to SIPRNet and ***(place any other network that may be connected).***

2. This IATO is valid for ***up to one year*** from the date of this letter. Final accreditation action is required before the expiration date of this IATO. This IATO will terminate sooner if there are any changes that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this IATO.

4. The undersigned accepts the risk for the operation of the ***(CINCs/Services/Agency's)*** system defined above.

Signature

Designated Approving Authority
CINCs/Services/Agency's

Mode of Operations Explanations

System High – A mode of operation wherein all users having access to the AIS posses a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

Dedicated – A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

Multi Level – A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access

approval for all data handled by the AIS.

Requirements for Consent to Monitor (CTM) Statement

- Date of statement
- Consent to Monitor heading
- Chairman Joint Chief of Staff instruction reference
- Statement acknowledging that DISA will conduct periodic monitoring of SIPRNet and consent to conducting initial and unannounced vulnerability assessments
- CINCs/Services/Agency's site name
- Designated Approving Authority (DAA)

Sample Consent to Monitor

Date

Consent to Monitor for SIPRNet, CCSD: _____

In accordance with the requirements of Chairman Joint Staff Instructions (CJCSI) 6211.02, Defense Information System Network and Connected Systems, 23 June 1993, and DISN Secret Internet Protocol Router Network (SIPRNet) connection requirements, we acknowledge that the Defense Information Systems Agency (DISA) will conduct periodic monitoring of SIPRNet. We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on our connected host systems to determine the security features in place to protect against unauthorized access or attack.

Signature

Designated Approval Authority (DAA)
CINCs/Services/Agency's name

Approval to Operate (ATO) Letter Requirements

The ATO grants approval for the operation of the system at hand. The letter will contain:

- The organization's letterhead and date of signature
- The specified security mode of operations and a specified data sensitivity or classification level
- Defined security safeguards (i.e., administrative, physical, personnel, COMSEC, emission, and computer security controls)
- System/Operating Applications (GCCS, DMS, CIS etc)
- A defined threat and stated vulnerabilities
- Stated interconnection to other systems
- A statement of acceptance of risk for the system
- A specified period of time (Up to three years maximum)
- A specified suite of hardware and software
- A specified operational environment
- Signature and signature block of the DAA

Sample ATO Letter

CINCs/Services/Agency's Letterhead
Address

Date

SUBJECT: Final Approval to Operate (ATO) the Secret Internet Protocol Router Network (SIPRNet) for CCSD: _____

Ref: (a) Accreditation Support Documentation

1. In accordance with the provisions of ***(CINCs/Services/Agency's)*** Instruction ***xxxx***, a final Approval to Operate (ATO) is hereby granted to the ***(CINCs/Services/Agency's)*** Network, located in building ***xxxx***, room ***xxxx, to include (list major applications), address***. This ATO is based upon a review of the information provided in reference (a). This ATO is valid for as long as the Baseline Security safeguards defined in the ***(CINCs/Services/Agency's specific security directives and guidelines)*** are implemented. This system is authorized to operate in the threat environment defined in reference (a) and with stated vulnerabilities as identified in the ***(CINCs/Services/Agency's Baseline Security Documents).*** The ATO system consists of ***(equipment list)***. This system is authorized to process ***(place maximum level of information being processed) in the (mode of operation)***. The ***(CINCs/Services/Agency's)*** network is connected to SIPRNet and ***(place any other network that may be connected)***.

2. This ATO is valid for ***up to three years*** from the date of this letter. Reaccredidation is required before the expiration date of this ATO. This ATO will terminate sooner if there are any changes that affects the security posture of the system. It is the responsibility of the senior official in charge of the system to ensure that any change in threat, vulnerability, configuration, hardware, software, connectivity, or any other modification is analyzed to determine its impact on system security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this ATO.

4. The undersigned accepts the risk for the operation of the ***(CINCs/Services/Agency's)*** system defined above.

Signature

Designated Approving Authority
CINCs/Services/Agency's

Requirements for Statement of Residual Risk

- CINCs/Services/Agency's Site letterhead
- Signature date
- Statement of Significant or Residual Risk to the CINCs/Services/Agency's System at the Users Location
- Assessment of the risk to confidentiality, integrity, availability, and accountability
- Assessment of the system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence
- Evaluation of operational procedures and safeguards with respect to their effectiveness and ability to offset risk at the CINCs/Services/Agency's Site
- Signature, full name, and title of Senior Site Official

Sample Statement of Residual Risk

CINCs/Services/Agency's
Address

Date

SUBJECT: Statement of Residual Risk for SIPRNet, CCSD: _____

1. The residual risk to the CINCs/Services/Agency's is (minimal or other). This assessment is based on evaluation of the known and presumed threats to the system, the vulnerabilities associated with the CINCs/Services/Agency's system, and all employed protective countermeasures.

2. The risk to system and data confidentiality, integrity, availability, and accountability is being maintained to an acceptable level. The vulnerabilities of the system with respect to the documented threat, ease of exploitation, potential rewards to the threat agent, and probability have been minimized by means of an aggressive Risk Management Program.

3. This Risk Management Program is based on a continual evaluation of the operational procedures and safeguards of the CINCs/Services/Agency's network to determine their effectiveness and ability to offset the defined risk at the CINCs/Services/Agency's site.

Signature

Chief, XX Branch
CINCs/Services/Agency

Requirements for Connectivity Description Diagram

Indicate and label the following devices, features, or information.

- (CINCs/Services/Agency's) associated devices including hubs, bridges, routers, guards, firewalls, major applications (i.e. – GCCS, DMS, CIS), gateways, modems, encryption devices, card readers, backup devices, room and bldg. number, surge protectors, UPS, and mechanical and electrical switches.
- Actual and planned interfaces to internal and external LANs or WANs (including backside connections).
- SIPRNet connections.
- The flow of information to, from, and through all connections.
- Router Port Number (RTRP), or CCSD number, if known and Host IP address(s).
- Diagrams must be clear and readable.

SIPRNet Access Assessment

Reference or DISA Package Number: _____
Command Communications Service Designator (CCSD): _____
Organization (CINC/Service/Agency/Contractor Name): _____
Location: _____
Date: _____
Plain Language Address (PLA)(Government Only): _____
POC and Phone number: _____
System or Network Name: _____
Premise Router IP Address: _____
Network IP Address Ranges: _____ _____
_____ _____ _____

This form is to be submitted with the initial request for connection and exercises. Additionally, this form is to be re-accomplished when there is a change to the approved configuration, recertification, or a change that affects the answers on file.

Circle or Highlight responses below.

Foreign National Access

#1 Yes No Foreign nationals, to include Integrated Officers (Foreign nationals in US positions), **have physical access to areas** where workstations **connect directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have access (escorted or unescorted) to the SIPRNet workstation areas, a Yes response is required.)

#2 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a network or subnet **connected directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have user accounts on SIPRNet workstations, a Yes response is required.)

#3 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a **separate network connected directly or indirectly** to SIPRNet.
(Example: A Non US network connected to a SIPRNet connection or using SIPRNet backbone as a transport layer to another Non US network, a Yes response is required.)

Contractor Access

#4 Yes No Uncleared contractors **have physical access to areas** where workstations on the organization network or its subnets **connected directly or indirectly** to the SIPRNet.
(Example: Uncleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to SIPRNet workstations, a Yes response is required)

#5 Yes No Uncleared contractors are **users** on workstations **connected directly or indirectly** to the SIPRNet.
(Example: Any contractor (Prime or Sub), US or Non-US, having a user account on the SIPRNet, a Yes response is required. Explain if the contractor is located within an U.S. Government, non-U.S. Government or Contractor facility.)

#6 Yes No Cleared contractors at a non-DoD facility are **users** on workstations **connected directly or indirectly** to the SIPRNet. Contract Number(s): _____.
(Example: Any contractor (Prime or Sub) at a non-DoD facility (including Contractor facilities) on a separate network such as an Educational Facility, a Yes response is required.)

#7 Yes No Reference question #6. Are there any uncleared personnel providing support under this contract.
(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical or services in support of the contract identified in number 6, a Yes response is required.

Network Connectivity - Include the Secret and Below Interoperability (SABI) Ticket Number (if Applicable) : _____

#8 Yes No The Organizational network, to include subnet(s) and workstation(s), connects to a network operating at any level other than Secret US Only, **with or without a high assurance guard or switches** in place.
(Example: A network operating at Unclassified But Sensitive, Unclassified, Confidential, Top Secret, NATO Secret, etc., a Yes response is required.)

This document and all attachments may become classified upon completion. Please follow your Security policies and procedures for the correct classification. If the document is unclassified it must be marked and handled as, "For Official Use Only".

_____

SIPRNet Access Assessment

If any of the above statements were answered with a **"YES"**, provide a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of foreign nationals, etc. and identify the Designated Approval Authority for that connection. Please be sure to sign and include the reference number on any and all attachments. Any questions may be directed to DISA, SIPRNet Connection Approval Office (SCAO) at (703) 882-1455, DSN: 381-1455.

If this document and its attachments are classified after completion, please call the SCAO at DSN: 381-2138 to coordinate a secure fax transmittal. You may also return it by registered mail to the following address:

John Staples
Defense Information Systems Agency, NS521
5275 Leesburg Pike (1N031F)
Falls Church, VA 22041

If the document and its attachments are unclassified after completion you may fax it to COMM (703) 882-2813 or DSN 381-2813.

CERTIFICATION: I certify that the information provided in this document and all attachments are accurate.

_____ OR

_____

Signature Block
Designated Approving Authority (DAA)

Signature Block
Information System Security Officer (ISSO)

DSS Addresses / Phone numbers

Northeast Region, DSS
New England Sector
Barnes Building 1040
495 Summer Street
Boston, Ma 02210-2192
COMM: (617) 451-4914
DSN: 955-4914
FAX: (617) 451-3052/4929

Northeast Region, DSS
Mid-Atlantic Sector
Kings Highway North
Cherry Hill, NJ 08034-1908
COMM: (609) 482-6505
DSN: 444-4030
FAX: (609) 482-0286

Central Region, DSS
Southwest Sector
106 Decker Court, Suite 200
Irving, TX 75062-2795
COMM: (214) 717-5228
FAX: (214) 717-0268

Central Region, DSS
Midwest Sector
610 S. Canal Street
Room 908
Chicago, IL 60607-4599
COMM: (312) 886-2436
FAX: (312) 353-1538

Pacific Region, DSS
Southern Sector
3605 Long Beach BLVD, Suite 405
Long Beach, CA 90807-4013
COMM: (310-595-7251
FAX: (310) 595-5584

Pacific Region, DSS
Northern Sector
Building 35, Room 114
The Presidio
San Francisco, CA 94129-7700
COMM:(415) 561-5608
FAX: (415) 561-2125

Capital Area, DSS
Hoffman Building
2461 Eisenhower Avenue
Alexandria, VA 22331-1000
COMM: (703) 325-9634
DSN: 221-9634
FAX: (703) 325-0792

Southeast Region, DSS
2300 Lake Park Drive
Suite 250
Smyrna, GA 30080-7606
COMM: (404) 432-0826
DSN: (697-6785
FAX: (404) 801-3300

UNCLASSIFIED

RUTUZYUW REDJDCA2006 1092052 MTMS-UUXX—XXXXXXX.1092101 318591

R182100Z APR 96
FM DISA WASHINGTON DC//D3//
TO CONUSMILNETSTA
CONUSDSNET1STA
AIG 8787
AIG 8791
CNO WASHINGTON DC//N6/N61/N62/N643//
CMC WASHINGTON DC//C4I/CS/CCT//
HQ USAF WASHINGTON DC//SC/SCM/AQPC//
DA WASHINGTON DC//DISC4/SAIS-ADM/DAMO-FD//
INFO SECDEF WASHINGTON DC//OASD:C3I//
JOINT STAFF WASHINGTON DC//J3/J6/J6S/J6T/J6V/J6Z//
ESC HANSCOM AFB MA//AVN//
HQ AFC4A SCOTT AFB IL//XPR//
CDR PM AWIS-CCS FT BELVOIR VA//SFAE-CC-AWT//
DISA EUR VAIHINGEN GE//EU/EU2/EU21//
DISA PAC WHEELER AAF HI//PC/PC2/PCC//
DISA CENTRAL COMMAND FWD//JJJ//
DISA CENTRAL COMMAND MACDILL AFB FL//DF//
VDRUSAISC FT HUACHUCA AZ//ASOP//
HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y441//
NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE MD//Q214//
NSACSS FORT GEORGE G MEADE MD//Y443//
ISPO ANNAPOLIS JUNCTION MD//JJJ//
COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//
COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
DNA WASHINGTON DC//COMP-1/NOCC//
DLA FT BELVOIR VA//CANAI//
DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
JOINT STAFF WASHINGTON DC//J6T/J8//
USCINCCENT MACDILL AFB FL//J6//
USSOCOM MACDILL AFB FL//J6//
USCINCPAC HONOLULU HI//J6//
HQ USSPACECOM CHEYENNE MOUNTAIN AS CO//J6//
USSTRATCOM OFFUTT AFB NE//J6//
USTRANSCOM SCOTT AFB IL//J6//
HQ SOUTHCOM QUARRY HEIGHTS PM//J6//
USACOM NORFOLK VA//J6//
USCINCEUR VAIHINGEN GE//J6//
CDRFORSCOM FT MCPHERSON GA//AFIS-O//
HQ DMA FAIRFAX VA//TSCEID.//
DMSSC WASHINGTON DC//EIT/TCO
DITCO SCOTT AFB IL//DTS//
DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN//

UNCLASSIFIED
UNCLASSIFIED

DISA SCOTT AFB IL//UNR/UNRSE/UNRSO//
DIA WASHINGTON DC//SC/SY/SY-3A/SY-3C//
NAVCOMTELSTA WASHINGTON DC//N912//
NAVCOMTELSTA PENSACOLA FL//N51/N32//

JSC ANNAPOLIS MD//INS//
ARNGRC ARLINGTON VA//NGB-AIS-SC//
CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB/DFAS-IN-MI//
CDRUSAISC COROZAL PM//ASNP-OPS//
DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//
DISA FLD OFC FT MCPHERSON GA//SANM//
DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
DISA FLD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC/D2/D21/D3/D34/D343/D381/D6/
JE/JT/WE/WEZ51/WE312//
BT
UNCLAS
OPER/CONUSMILNETSTA 03/96/CONUSDSNET1STA 02/96//
SUBJ/DEADLINE EXTENSION TO DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//
REF/RMG/DISA WASHINGTON DC/D/121713Z DEC 95//
POC/KYRA JENKINS/RM1/D343/LOC:DISA WASH/TEL:DSN 653-8041/TEL:COMM (703)735-8041//
RMKS/1.REF MESSAGE OUTLINES CONNECTION REQUIREMENTS FOR EXISTING AND POTENTIAL SIPRNET SUBSCRIBERS. THESE REQUIREMENTS ARE CRUCIAL FOR ENSURING OVERALL NETWORK SECURITY INTEGRITY AND TO FACILITATE FINAL ACCREDITATION OF THE SIPRNET.
2. FOR ALL EXISTING SIPRNET CONNECTIONS: AN INTERIM APPROVAL TO CONNECT TO SIPRNET IS HEREBY EXTENDED UNTIL 31 JUL 1996, AT WHICH TIME ALL REQUIREMENTS OUTLINED IN REF MESSAGE MUST BE COMPLETED. THIS EXTENSION IS DUE TO A SUBSTANTIAL NUMBER OF CUSTOMERS WHO DID NOT RECEIVE DISA'S ORIGINAL MESSAGE.
3. ALL CURRENT AND PROSPECTIVE SIPRNET CUSTOMERS ARE TO SUBMIT A SYSTEM PACKAGE WITH REQUIRED DOCUMENTATION TO DEFENSE INFORMATION SYSTEMS AGENCY. ATTN: D343 (RM1 KYRA JENKINS), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087. FAILURE TO COMPLY MAY RESULT IN SERVICE DISRUPTION OR DENIAL OF CONNECTION APPROVAL. TO FACILITATE PACKAGE PROCESSING. REQUEST CUSTOMEWRS INCLUDE THE ASSIGNED COMMAND AND CONTROL SERVICE DESIGNATOR (CCSD) OR IP ADDRESS FOR EACH SIPRNET CONNECTION UNDER THEIR RESPONSIBILITY.

UNCLASSIFIED
UNCLASSIFIED

4. RECIPIENTS ARE REQUESTED TO ENSURE WIDEST DISSEMINATION OF THIS MESSAGE.
5. DISA POC IS RM1 KYRA JENKINS, DSN 653-8041/COMM 703-735-8041/EMAIL: JENKINSK@NCR.DISA.MIL.//
BT

Note** Change reference to RM1 Jenkins to Mr. John Staples (DSN) 653-3236 (Comm) 703-735-3236

UNCLASSIFIED

U N C L A S S I F I E D

ROUTINE

R 161945Z APR 97

FM JOINT STAFF WASHINGTON DC//VJ6//

TO CINCUSACOM NORFOLK VA//J2/J3/J6//

USCINCCENT MACDILL AFB FL//CCJ2/CCJ3/CCJ6//
USCINCSOC MACDILL AFB FL//SOJ2/SOJ3/SOJ6//
USCINCPAC HONOLULU HI//J2/J3/J6//
USCINCSPACE PETERSON AFB CO//J2/J3/J6//
USSTRATCOM OFFUTT AFB NE//J2/J3/J6//
USCINCTRANS SCOTT AFB IL//TCJ2/TCJ3/TCJ6//
USCINCSO SCJ6 QUARRY HEIGHTS PM//SCJ2/SCJ3/SCJ6//
USCINCEUR VAIHINGEN GE//ECJ2/ECJ3/ECJ6//
CNO WASHINGTON DC//N6/N61/N62/N643/N2/N3//
CMC WASHINGTON DC//C4I/CS/PPO/POC//
HQ USAF WASHINGTON DC//SC/SCM//
SAF WASHINGTON DC//AQI/AQII/AQPC//
DA WASHINGTON DC//DISC4/SAIS-ADM/DAMO-FD//
OSI WASHINGTON DC//SO/DR/CC//
FINCEN VIENNA VA//
FLTINFOWARCEN NORFOLK VA//N6/N62//
NAVLANTMETOC DET KEFLAVIK IC//JJJ//
COMICEDEFOR KEFLAVIK IC//J6//
USCS BAY ST LOUIS MS//
AEDC ARNOLD AFB TN//IN//
123IS LITTLE ROCK AFB AR//IN//
AFMC CSO WPAFB OH//SCMF//
DET 2 696 IG WPAFB OH//RMC//
USCINCCENT MACDILL AFB FL//CCJ6-C//
DIA WASHINGTON DC//SY//
COMMARCORSYSCOM QUANTICO VA//NOC/PMICS//
COMDR FORSCOM FT MCPHERSON GA //AFIN-RD/AFIN-ID/
/AFIS-OP/AFZK-IMP//
HQ AFSPC PETERSON AFB CO//LGS//
NATIONAL DRUG INTELLIGENCE CENTER JOHNSON PA//
DEA HQS WASHINGTON DC//SIOM//
CDRUSACAA BETHESDA MD //CSCA-CST//
AFPCA WASHINGTON DC//GAC/OPSD//

UNCLASSIFIED

BBN SYSTEMS & TECHNOLOGIES CAMBRIDGE MA//MS6/4D//
CDRCECOM FT MONMOUTH NJ //AMSEL-MI-I//
COGARD COMMSTA MIAMI FL//
NAVOCEANO STENNIS SPACE CENTER MS//N624//
DPAC ANDREWS AFB MD//CH//
18 ABNCORPS FT BRAGG NC//AFZA-GT-OCR//
CDRICORPS FT LEWIS WA//AFZH-OO//
CDRIIICORPS FT HOOD TX//G2/G3/G6//
CDRVCORPS FRANKFURT GE//G2/G3/G6//
621AMOS MCGUIRE AFB NJ //IN//
COMSCLANT BAYONNE NJ//N6/N65/N652//
FITCPAC SAN DIEGO CA//02//
RUEHBK/AMEMBASSY BANGKOK//DEA//

RUEHWN/AMEMBASSY BRIDGETOWN//DEA//
NAVCOMTELSTA PENSACOLA FL//N32//
CCGDSEVEN MIAMI FL//OC/OI//
DISA WASHINGTON DC//D64//
DNA WASHINGTON DC//NOCC//
COMNAVSPACECOM DAHLGREN VA//N621//
CDR1111THSIGBN FT RITCHIE MD//ASQY-SRP-S/ASQY-SRP-N//
COMNAVRESFOR NEW ORLEANS
LA//N321/WE337/WE345/WE3452.DB//
INFO SECDEF WASHINGTON DC//OASD:C3I//
JOINT STAFF WASHINGTON
DC//J3/J33/CSOD/J6/J6S/J6T/J6V/J6Z/J2//
ESC HANSCOM AFB MA//AVN//
HQ AFCA SCOTT AFB IL//SYNE/XPR//
CDR PM AWIS-CCSFT BELVOIR VA //SFAE-CC-AWT//
DISA EUR VAIHINGEN GE//EU/EU2/EU21//
DISA PAC WHEELER AAF HI//PC/PC2/PCC//
DISA CENTRAL COMMAND FWD//JJJ//
DISA CENTRAL COMMAND MACDILL AFB FL//DF//
CDRUSAISC FT HUACHUCA AZ//ASOP//
HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
DIRNSA FT GEORGE G MEADE MD //Q11/Q21/Y414/Y441//
NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE
MD//Q214//
NSACSS FORT GEORGE G MEADE MD//Y443//
ISPO ANNAPOLIS JUNCTION MD//JJJ//
COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//
COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
DNA WASHINGTON DC//COMP-1/NOCC//

UNCLASSIFIED
UNCLASSIFIED

DLA FT BELVOIR VA//CANAI//
DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
CDRFORSCOM FT MCPHERSON GA//AFIS-O//
HQ DMA FAIRFAX VA//TSCEID//
DMSSC WASHINGTON DC//EIT/TCO//
DITCO SCOTT AFB IL//DTS//
DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN//
DISA SCOTT AFB//UNR/UNRSE/UNRSO//
DIA WASHINGTON DC//SC/SY-3A/SY-3C//
NAVCOMTELSTA WASHINGTON DC//N912//
NAVCOMTELSTA PENSACOLA FL//N51/N32//
JSC ANNAPOLIS MD//INS//
ARNGRC ARLINGTON VA//NGB-AIS-SC//
CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//DFAS-IN-MI//
CDRUSAISC COROZAL PM//ASNP-OPS//
DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//

DISA FLD OFC FT MCPHERSON GA//SANM//
DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
DISA FLD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC//
DISA WASHINGTON DC//D2/D21/D3/D36/D361/D3613/D381//
DISA WASHINGTON DC//D6/JE/JT/WE/WEZ51/WE312//
AIG 8791
UNCLAS
SUBJ/DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//
REF/A/MSG/DISA WASHINGTON DC/D/121713ZDEC95, SAME SUBJECT//
REF/B/MSG/DISA WASHINGTON DC/D3/182100ZAPR96/SUBJ:DEADLINE EXTENSION TO DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//
AMPN/REF A ESTABLISHED A DEADLINE FOR SIPRNET SUBSCRIBERS TO MEET SPECIFIC REQUIREMENTS CRUCIAL TO THE OVERALL NETWORK SECURITY OF THE SIPRNET. REF B EXTENDED THE DEADLINE FOR OPERATIONAL SIPRNET CUSTOMERS TO SUBMIT THEIR SYSTEM SECURITY PACKAGES TO 31 JUL 1996.//
POC/TINA HARVEY/MAJ/J6T/LOC:JOINT STAFF/TEL:DSN 223-1747/TEL:COMM (703) 693-1747/EMAIL:HARVEYTM@JS.PENTAGON.MIL//
RMKS/1. IN THE INTEREST OF PROTECTING THE SIPRNET AND ITS SUBSCRIBERS, ALL SIPRNET SUBSCRIBERS THAT DIRECTLY CONNECT TO SIPRNET

MUST COMPLETE SYSTEM SECURITY PACKAGES IAW REF A. DISA IS ASSIGNED THE RESPONSIBILITY FOR SIPRNET CONNECTIVITY AND ACCREDITATION AND WILL NOT CONNECT NEW SUBSCRIBERS TO SIPRNET WITHOUT THESE PACKAGES. REF B REQUIRED ALL SIPRNET SUBSCRIBERS HAVE THESE PACKAGES SUBMITTED

TO DISA NLT 31 JUL 96.

2. TO DATE, ONLY 194 OF THE 382 SYSTEMS CURRENTLY CONNECTED HAVE COMPLETED SYSTEM SECURITY PACKAGES. COMPLIANCE IS CRUCIAL FOR ENSURING OVERALL NETWORK SECURITY. TO ASSIST IN COMPLIANCE, JOINT STAFF/J6T MET WITH SERVICE POINTS OF CONTACT ON 10 JAN 97 AND CO-HOSTED A MEETING WITH DISA FOR AGENCIES ON 18 FEB 97 TO AGAIN OUTLINE REQUIREMENTS AND ISSUES. IN ORDER TO DOCUMENT PROGRESS TOWARD RESOLUTION, JOINT STAFF/J6T WILL PERIODICALLY SEND OUT FOLLOW UP MESSAGES TO CINCS, SERVICES AND AGENCIES IDENTIFYING NON-COMPLIANT SYSTEMS UNDER THEIR RESPONSIBILITY.

3. ALL EXISTING SIPRNET SUBSCRIBERS WHO HAVE NOT YET COMPLIED WITH THE REQUIREMENTS IN REFS A AND B MUST CONTACT DISA/D3613 IMMEDIATELY AND SUBMIT SYSTEM SECURITY PACKAGES TO DISA AS OUTLINED IN REF A. DUE DATE FOR ALL PACKAGES CURRENTLY OUTSTANDING IS 15 JUL 97. DISA POCS ARE LISTED IN PARAGRAPH 4 OF THIS MESSAGE. DISA HAS DEVELOPED A PACKAGE THAT PROVIDES DETAILED INSTRUCTIONS AND EXAMPLES OF SYSTEM SECURITY DOCUMENTATION THAT WILL BE MADE AVAILABLE UPON REQUEST. IF

SYSTEM SECURITY PACKAGES CANNOT BE COMPLETED BY 15 JUL 97, FORMAL WRITTEN REQUESTS FOR AN EXTENSION ARE REQUIRED. SEND BY MESSAGE TO: DISA WASHINGTON DC//D3613//, BY MEMORANDUM TO: DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D3613 (JOHN STAPLES), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087, FAX: DSN 653-8482/COMM 703-735-8482. REQUESTS FOR EXTENSION MUST INCLUDE: ORGANIZATION POINT OF CONTACT, PROJECTED DATE OF PACKAGE SUBMISSION, ASSIGNED SYSTEM COMMAND AND CONTROL SERVICE DESIGNATOR (CCSD) AND SIPRNET IP ADDRESS FOR EACH DIRECT SIPRNET CONNECTION UNDER THEIR RESPONSIBILITY. APPROVAL WILL BE ON A CASE BY CASE BASIS.
4. RECIPIENTS ARE REQUESTED TO ENSURE WIDEST DISSEMINATION OF THIS MESSAGE. IF THERE ARE ANY QUESTIONS, PLEASE CONTACT DISA/D3613 POCS
A. JOHN STAPLES/DSN: 653-3236/COMM: 703-735-3236/EMAIL STAPLESJ@NCR.DISA.MIL/MAIL: DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D3613 (MR. JOHN STAPLES), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087, OR
B. JIM NOSTRANT/DSN: 653-3238/COMM: 703-735-3238/EMAIL: NOSTRANJ@NCR.DISA.MIL//

BT