SIPRNet Connection Questionnaire

SCQ

This form must be submitted with all (including exercise, tactical and contingency) requests for connection to the SIPRNet. An updated copy of this form must be submitted when there is a change to the enclave configuration, certification, and/or a change that affects one or more answers on the previously submitted SCQ (if applicable).

Date: _____

DISA Package Number (Assigned by the DISA CAO): _____

Classified Network Command Communications Service Designator(s) (CCSD) / Circuit Identifier (e.g., COINS), and/or Satellite Access Request (SAR/GAA Nr.): _____

Collocated NIPRNet CCSD(s): _____

Organization (Combatant Command/Service/Agency/Sub-Agency/Contractor Name): _____

_____

Organization Address (DAA Mailing Address):

_____

Point of Presence (POP) Location (Bldg, Room, Base/Post/Camp/Mobile Platform): _____

_____

Organizational DMS Address: _____

Enclave/Network DAA (Name, Rank/Grade): _____

Enclave/Network DAA Phone Number (Commercial, DSN): _____

Enclave/Network DAA SIPRNet Email Address: _____

Enclave/Network DAA NIPRNet Email Address: _____

Technical POC: (Name, Rank/Grade): _____

Technical POC Phone Number (Commercial, DSN): _____

Technical POC SIPRNet E-mail Address: _____

Technical POC NIPRNet E-mail Address: _____

Administrative POC (Name, Rank/Grade): _____

Administrative POC Phone Number (Commercial, DSN): _____

Administrative POC SIPRNet Email: _____

Administrative POC NIPRNet Email Address: _____

Fax Number (Secure and Unsecure): _____

*CNDSP Organization*_____

CNDSP POC (Name, Rank/Grade, Service): _____

*CNDSP POC Phone Number (Commercial, DSN):*_____

CNDSP POC SIPRNet Email: _____

CNDSP POC NIPRNet Email: _____

CC/S/A IA POC (Name, Rank/Grade): _____

CC/S/A IA POC Phone Number (Commercial, DSN): _____

CC/S/A IA POC SIPRNet Email: _____

CC/S/A IA POC NIPRNet Email: _____

*System or Network Name:*_____ **Premise Router IP Address(s) :*_____

**Network IP Address Ranges:* _____ _____

_____ _____ _____

_____ _____ _____

**Rel IP Address Range(s) (if applicable):* _____ _____

*****NOTE: IAW the Network Infrastructure STIG, IP Address Registration Using RFC1918 addresses (non-routable) and network address translation (NAT) on the SIPRNet is prohibited. Full SIPRNet Registered IP addresses MUST be entered on this form. IP notation such as X.X.15.1 is not acceptable. Failure to comply will cause a delay in the processing of your connection request.

This questionnaire and all attachments may become classified upon completion. Please follow your local and higher headquarters' security policies and procedures for assigning the classification and subsequent handling. If the questionnaire is unclassified, it must be marked and handled as "Unclassified // For Official Use Only".

_____

DAA/IAM Initials

DISN Classified Network Package Number:_____ CCSD:_____

Circle responses below.

Combatant Command, Service, or DOD Agency Sponsor /OSD Approval
(Mandatory for Non-DOD (e.g., Contractor or other Non-DOD entity) and Foreign National Activities)

#1 Yes No Does this connection support a Non-DOD or Foreign National User Connection?
(Reference CJCSI 6211.02D, Enclosure D – If "Yes", the DOD sponsoring agency must submit a request for connection memorandum to OASD (NII) / DOD CIO for approval. The memorandum template can be viewed / downloaded at http://www.disa.mil/connect/library/index.html. A copy of the OASD approval memorandum must be provided to the CAO with the Connection Approval package.)

Non-DOD Access & Connections (Contractor or Other non-DoD activity) Facility

#2 Yes No N/A Do any uncleared personnel have physical access to Non-DOD facility areas where work centers, terminals, or equipment connect directly or indirectly to the SIPRNet?
(Example: If any personnel, either in support of a Government/Non-DOD Government contract or maintenance support [to include cleaning personnel], have access to areas where classified workstations are located, a "Yes" response is required.)

#3 Yes No N/A Are cleared contractors at a non-DOD facility **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) that connects to the SIPRNet or on a separate network such as an Educational Facility that is logically or physically connected/interfaced to the users network, a "Yes" response is required.)

Foreign National Access

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

#5 Yes No Are Foreign Nationals, to include Liaison Officers, **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 classified workstations or via a REL implementation configuration, a "Yes" response is required.)

#6 Yes No Has the Foreign National access been provided in accordance with the Embedded REL User Enclave, Technical Implementation Instructions?
(Implementation must be IAW the Embedded REL User Enclave, TII, reference SIPRNet website: http://www.ssc.smil.mil – Policy/Guidance & Documentation – Sharing.)

DOD Facility Access & Connections

#7 Yes No N/A Do Non-DOD personnel have physical access to facility areas where workstations, terminals, or equipment connect directly or indirectly to the SIPRNet?
(Example: If Non-DOD personnel, either in support of a DOD Government contract or maintenance support, to include cleaning people, have access to areas where classified workstations are located, a "Yes" response is required)

#8 Yes No N/A Do any uncleared personnel have physical access to facility areas where work centers, terminals, or equipment connect directly or indirectly to the SIPRNet?
(Example: If any uncleared personnel, either in support of a DOD Government contract or maintenance support, to include cleaning people, have access to areas where SIPRNet workstations are located, a "Yes" response is required)

DISN Classified Network Package Number:_____**CCSD:**_____

Network Connectivity

#9 Yes No ○ ○ Does this connection support a Cross Domain Solution (CDS)?
If Yes, please provide your IP Address(s) _____

(Reference CJCSI 6211.02D, Enclosure C and D – If "Yes", the DOD sponsoring agency must enter the Joint Staff priority level and date of validation in the Phase I tab of the SGS CDS record.)

#10 Yes No ○ ○ Is the activity's classified network, to include subnet(s) and systems/devices, physically/logically connected or interfaced to a network or platform operating at any level other than Secret US Only? This includes tunneling, switches, or connections **with or without high assurance guards** in place? Include the Cross Domain Solution (CDS) Ticket Number (if Applicable) : _____

(Example: If a network is operating at Sensitive but Unclassified, Unclassified, Confidential, Top Secret, NATO Secret, REL, etc., and has a physical or logical interface/connection with the SIPRNet, a "Yes" response is required. This includes configurations where the other network is cryptographically isolated (i.e., GRE)

#11 Yes No ○ ○ Is the activity's classified network, to include subnet(s) and systems/devices, physically/logically connected or interfaced to a network or platform operating at another Secret Level? This includes tunneling, switches, or connections **with or without high assurance guards** in place? Include the Cross Domain Solution (CDS) Ticket Number (if Applicable) : _____

(Example: If a network operating at Secret Level, e.g., SDREN, JTEN, DMON, etc., and has a physical or logical interface/connection with the SIPRNet, a "Yes" response is required. This includes configurations where the other network is cryptographically isolated (i.e., tunneled).)

Wireless Connectivity

#12 Yes No ○ ○ Does the activity's classified network (configuration/architecture) include wireless technology?

(Example: If wireless technology is/has been implemented on the user's enclave, the device(s), configuration guidance, and topology must be included in the explanation.)

Classified Mobile Connectivity

#13 Yes No ○ ○ Does the activity's classified network (configuration/architecture) include classified secure mobile technology?

(Example: If mobile technology (e.g., SME-PED) is/has been implemented on the user's enclave, the device(s), configuration guidance, and topology must be included in the explanation.)

Ports & Protocol Registration

#14 Yes No ○ ○ Has the user registered all of the network systems on this connection with DOD Ports, Protocols and Services Management (PPSM) System, IAW DODI 8551.1? A "No" response requires an explanation of when registration will be accomplished. A request to connect to the DISN network/service will not be approved until PPSM registration is accomplished.

(Explanation: All DISN activities are required to comply with this directive when connecting to a DOD network.)

SIPRNet IT Registration

#15 Yes No ○ ○ Has the user registered all of the network systems/devices on this connection IAW CJCSI 6211.02D?

(Explanation: DoD policy requires that partners register their IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil. An enclave/network may also be registered in the SIPRNet IT Registry, by first requesting an account to the application at https://arm.osd.smil.mil. Once you have an account, the link to the SIPR IT Registry is: http://osdext.osd.smil.mil/sites/dodcio/itregistry/default.aspx. A "No" response requires an explanation of when registration will be accomplished.)

Boundary Protection

#16 Yes No ○ ○ Has your enclave deployed at the enclave boundary an approved Firewall and IDS device IAW DoD guidance? Customers shall provide the device make and model and software version on the network topology diagram. A "No" response requires Plan of Action and Milestones (POA&M), with an explanation of when approved products will be deployed.

(Explanation: All SIPRNet activities are required to use NIAP validated devices (Ref - http://www.naip-ccevs/org/cc-sceme/vpl) to protect their enclaves (Ref - DODI 8500.2E) and configure them IAW the Network Infrastructure STIG (Ref - http://iase.disa.mil/stigs/stig/index.html)

DISN Classified Network Package Number:_____ **CCSD:**_____

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

X _____

Signature Block
Designated Approving Authority (DAA)
(or DAA approved IAM)

If signed by the DAA approved IAM, complete the following contact information:

IAM (Name, Rank/Grade): _____
*IAM Phone Number (Commercial, DSN):*_____
IAM SIPRNet Email Address: _____
IAM NIPRNet Email Address: _____

If any of the above statements were answered with a **"YES"** (with the exception of questions 14-16), a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of foreign nationals, etc., must be provided. Please be sure to initial/sign all pages and include the reference package number on any and all attachments. Any questions may be directed to DISN, Connection Approval Office (CAO) at (301) 225-2901, DSN: 375-2901.

If this questionnaire and its attachments are classified after completion, you may send it via e-mail with your package to Disa.meade.ns.mbx.ccao@mail.smil.mil or via registered mail to the following address:

DISA
ATTN: NSC1/CAO
P.O. Box 549
Ft. Meade, MD 20755-0549

When data is entered on this questionnaire, as a minimum, it must be marked and handled as "For Official Use Only". IAW DISAC 300 115-3, Defense Information System Network (DISN) Secret Internet Protocol Routing Network (SIPRNet) Security Classification Guide, 25 October 2007, Enclosure 4 3.1.1, the following type of information is UNCLASSIFIED//FOUO: "Databases, documents, or graphics that provide the following information either as individual items or in combination: Customer Identification, System Identification, Wide Area Network (WAN) Identified as SIPRNet, SIPRNet Node Identification, SIPRNet Port Identification, SIPRNet IP Address." .