NISP SIPRNet Circuit Approval Process
August 2016 v2.4

Purpose

The NISP SIPRNet Circuit Approval Process (NSCAP) was developed to provide step-by-step guidance for cleared contractors and their sponsors with contractual requirements to establish a connection to the SIPRNet. The NSCAP is based upon established policy and guidance for Non-DoD DISN connections as documented in the DISA Connection Process Guide (CPG).

Roles and Responsibilities

PARTICIPANT	RESPONSIBILITIES
Defense Security Service (DSS)	• DAA/AO for Information Systems (IS) used to process classified information in the National Industrial Security Program (NISP) • Process and review System Security Plans (SSP) • Performs on-site assessment and validates certification of IS.
Defense Information Systems Agency (DISA)	• Responsible for DoD Information Network (DoDIN) circuits and oversight per CJCSI 6211.02D • Process Connection Approval Packages (CAP) and make connection decisions (IATC/ATC) • Publish DISN Connection Process Guide (CPG)
Office of the Assistant Secretary of Defense for Networks and Information Integration (DOD CIO)	• Final approval authority for all Non-DOD DISN Connection Validation/Revalidation requests in support of sponsor's mission.
Government Sponsor/Owner of contractor connection(s)	• Validate the requested DISN connection is required to support a mission • Provide funding for circuit and any other required services or tools for contractor connection SIPRNet (i.e. CNDSP, email, DNS, HBSS) connection in order to maintain DoD IA compliance

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

Process Overview

A. Non-DOD Validation of New DISN Connections:

1. Government Sponsor completes and submits the Non-DOD DISN Connection Validation Letter (Validation Letter) to disa.meade.ns.mbx.siprnet-management-office@mail.mil (download template http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide/DISN-Service-Appendices/Non-DoD-DISN-Connection-Validation). DISA SIPRNet Service Manager Office (SSMO) reviews the Validation Letter and network topology to determine whether the proposed DISN solution is appropriate. If so, the SSMO forwards the Validation Letter to Sponsor's Service/Agency for endorsement.

2. Government Sponsor's Service/Agency forwards the Service/Agency endorsed (2nd endorsement) Validation Letter to DOD CIO, Governance Directorate for review/approval.

3. DOD CIO reviews the Government Sponsor Validation Letter. If the connection request is approved, DOD CIO will sign an approval memo and email it to DISA SMO, DSS, and the Government Sponsor.
   - Prior to DOD CIO validating a circuit request, the Government Sponsor must ensure the connection is aligned with a DOD accredited Computer Network Defense Service Provider (CNDSP) via an MOU/A that is funded/resourced. See CNDSP section below for more information.

4. Government Sponsor initiates order of SIPRNet circuit through DISA Direct Order Entry (DDOE) process, https://www.disadirect.disa.mil/products/asp/welcome.asp. (PKI required) Or contact DISN Global Support Center (DGSC) 800-554-3476.

5. Contractor prepares SSP and required documentation in accordance with the DSS Industrial Security Field Operations (ISFO) Process Manual or Risk Management Framework (RMF) when applicable, for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM). DSS accreditation will not exceed 3 years or contract expiration date.

   Required documentation to be submitted through ODAA Business Management System (OBMS)

   - The Non-DOD DISN Connection Validation Letter endorsed by the Government Sponsor, the DISA SSMO, and the Service/Agency validation official.
   - DOD CIO connection approval memo (if available)
   - Consent To Monitor (CTM) memorandum with Government Sponsor's signature.

- Statement of Residual Risk with contractor signature.
- SSP and IS Profile
- Copy of MOU/A or contract signed by CNDSP and sponsor (the MOU/A must be funded/resourced)
- Evaluated Assurance Level (EAL) certificates validating at least EAL-4 Firewall and EAL-2 IDS. (http://www.niap-ccevs.org/vpl); DISA Approved Products List (APL)
- Risk Acknowledgement Letter(s) (if applicable)
- ***Classified POA&Ms are coordinated with DSS ISSP and submitted via secure channels only.***

6. Sponsor registers connection information in the following systems;

    a. **SIPRNet IT Registry**; https://arm.osd.smil.mil.
    b. **Register SIPRNet Support Center (SSC)** For more information sponsors shall contact DOD Network Information Center (NIC) at 800-582-2567 or www.ssc.smil.mil (SIPR)
    c. **Ports, Protocols, and Services Management (PPSM);** all network/systems ports, protocols, and services must be registered appropriately. Sponsors shall contact (301) 225-2904, dod.ppsm@mail.mil or ppsm@disa.smil.mil (SIPR) for more information. Document the PPSM tracking ID number; you will need to enter the number into SGS.
    d. **SIPRNet GIAP System (SGS)**; sponsor must obtain an account and register their circuit appropriately. See Additional Guidance section of this document for detailed information. https://giap.disa.smil.mil/gcap/home.cfm

7. Contractor/Sponsor submits Connection Approval Package (CAP) to DISA Classified Connection Approval Office (CAO) by uploading all documentation to the SIPRNet GIAP System (SGS).
    a. See instructions on how to obtain a SGS account at the Additional Guidance section of this document. Once package is verified, Interim Authorization to Test (IATT) will be granted by DISA and initiate burn-in testing by DISA Implementation, Testing, and Acceptance (IT&A).

8. After burn-in and remote compliance vulnerability scan by DISA IT&A, DISA CAO makes a connection decision and customer/sponsor is notified. If CAP is approved sponsored circuit will receive Interim Approval to Connect (IATC) or Approval to Connect (ATC) as appropriate.

9. Complete the Disclosure Authorization (DA) form and have signed by sponsor. Submit the submitted form to the following email: Disa.scott.global.mbx.smc-contractor@mail.mil

    a. The DISA Web Content Filtering Service (WCFS) will receive the DA request and built the contractor proxy accordingly.

Termination/Disestablishment – Per ISFO PM, when the contractor SIPRNet IS has come to the end of its usefulness due to end of contract or program, etc. accreditation for the IS will need to be withdrawn. The sponsor shall then disconnect the service by contacting DISA DDOE (see step #4 above).

NISP contractors shall note **expiration dates of DSS ATO and DISA ATC. Per ISFO PM, it is the contractor ISSM's responsibility to submit plans for reaccreditation at least **90 days** of expiration to allow Office of Designated Approving Authority (ODAA) to review the plan. Always update DISA CAO with new DSS accreditation letters. The sponsor/contractor shall work directly with DISA to revalidate circuit appropriately with enough time to prevent disconnection because of an expired IATC/ATC.

B. Non-DOD Revalidation of Existing Connections:

1. If there is a change in sponsor, mission, requirement, contract or location then full revalidation is required. The Government Sponsor completes and submits the Non-DOD DISN Connection Revalidation Letter to disa.meade.ns.mbx.siprnet-management-office@mail.mil.
    - Note; revalidation review is not required unless there is a change to the mission, contract, physical location (e.g. CAGE Code), or sponsor. Any one single change will require a full revalidation through DISA SSMO to the CC/S/A Validation Official to DoD CIO. Revalidations for contract extensions (e.g. 30 days, 90 days, one year) no longer require revalidation reviews by DISA SSMO.

2. DISA SIPRNet Service Manager Office (SSMO) reviews the Validation Letter and network topology to determine whether the proposed DISN solution is appropriate. If so, the SSMO forwards the Validation Letter to Sponsor's Service/Agency for endorsement.

3. Government Sponsor's Service/Agency forwards the Service/Agency endorsed (2nd endorsement) Validation Letter to DOD CIO, Governance Directorate for review/approval.

4. DOD CIO reviews the Government Sponsor Validation Letter. If the connection request is approved, DOD CIO will sign an approval memo and email it to DISA SMO, DSS, and the Government Sponsor.

5. Contractor prepares SSP and required documentation for reaccreditation in accordance with the DSS Industrial Security Field Operations (ISFO) Process Manual for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM). DSS accreditation will not exceed 3 years or contract expiration date.

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

Required documentation to be submitted to DSS OBMS:

- Non-DOD DISN Connection Revalidation Letter endorsed by the Government Sponsor and DISA SSMO
- Consent To Monitor (CTM) memorandum with sponsor signature.
- Statement of Residual Risk with contractor signature.
- SSP and IS Profile
- Copy of MOU/A or contract signed by CNDSP and sponsor (the MOU/A must be funded/resourced)
- Evaluated Assurance Level (EAL) certificates validating at least EAL-4 Firewall and EAL-2 IDS. or DISA Approved Products List (APL)
- Risk Acknowledgement Letter(s) (if applicable)
- ***Classified POA&Ms are coordinated with DSS ISSP and submitted via secure means only.***

6. Contractor/Sponsor submits updated Connection Approval Package (CAP) to DISA Classified Connection Approval Office (CAO) by uploading all documentation to the SIPRNet GIAP System (SGS) located on SIPRNet at https://giap.disa.smil.mil DISA CAO no longer accepts CAP via email and will only accept the documentation via SGS, see instructions on how to obtain a SGS account at the Additional Guidance section of this document.

7. DISA CAO makes a decision, customer/sponsor is notified. If CAP is approved sponsored circuit will receive IATC/ATC.

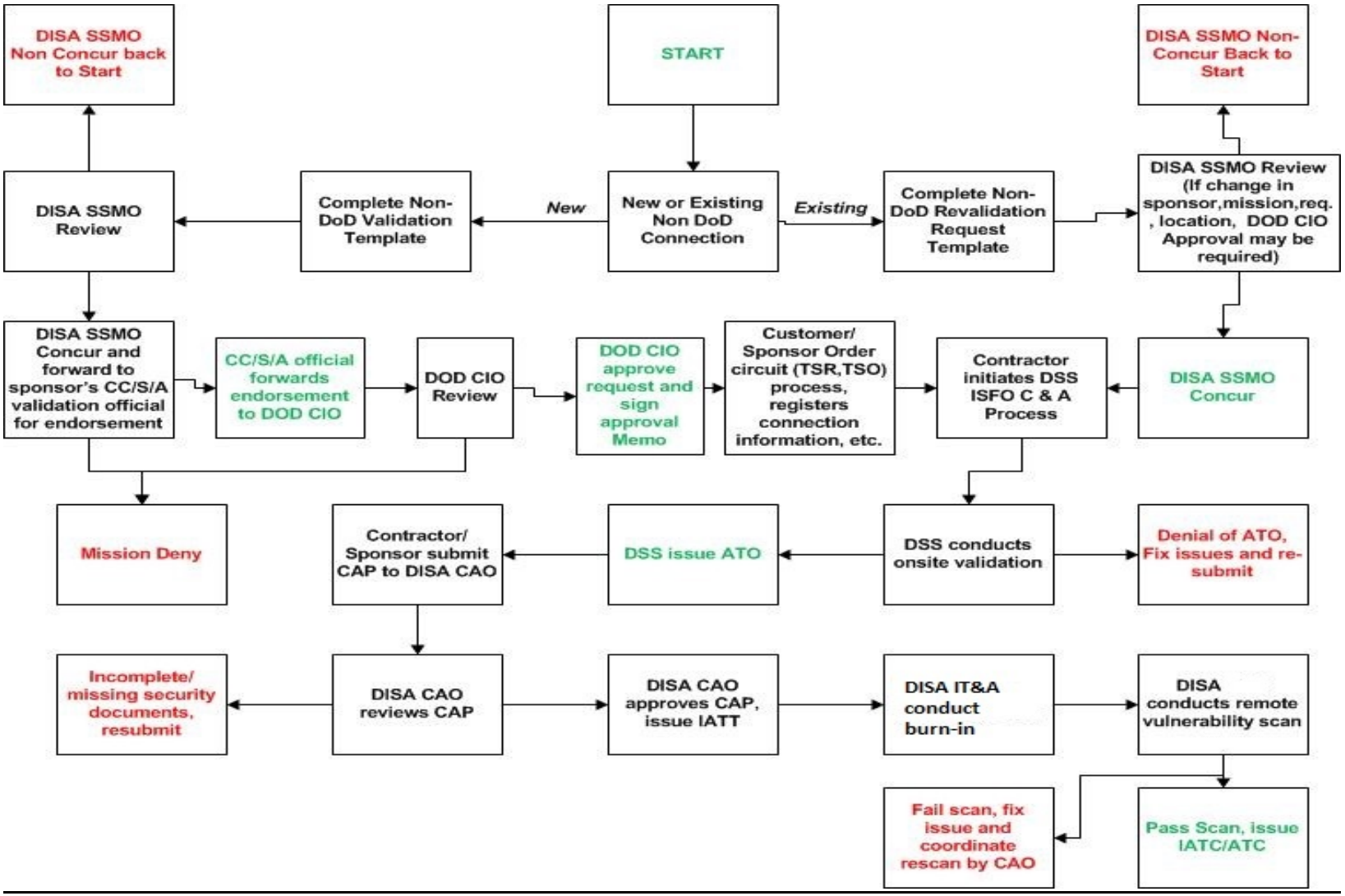
Termination/Disestablishment – Per ISFO PM, when the contractor SIPRNet IS has come to the end of its usefulness due to end of contract or program, etc. accreditation for the IS will need to be withdrawn. The sponsor shall then disconnect the service by contacting DISA DDOE.

DISA Connection Approval FAQ's: http://disa.mil/Services/Network-Services/Enterprise-Connections/FAQs/Connection-Approval-FAQs

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

Process Flow



Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

NISP SIPRNet Circuit Approval Process
August 2016 v2.4
Additional Guidance

Certification and Accreditation

DSS and DISA have agreed on a Memorandum of Agreement (MOA) that defines the roles, responsibilities, and relationships between DSS and DISA for contractor classified information systems connecting to the Secret Internet Protocol Router Network (SIPRNET). As a result of the MOA, NISP contractors with DoD CIO approval to connect information systems to the SIPRNet are required to implement enhanced security measures beyond the NISPOM. The enhanced security controls shall be implemented prior to requesting certification and accreditation from DSS and fully documented in the (M) SSP. Compliance with the DoD policies is required throughout the system's lifecycle. Failure to implement the enhanced security measures may add an additional level of risk deemed unacceptable by the DAA of the IS (DSS) and connecting network (DISA) resulting in disconnection of the network by a withdrawal or termination of an accreditation.

Government Sponsor Responsibilities:

1. Validate the requested contractor connection to DISN is required to support a DOD mission

2. Provide funding for circuit and any other required services for contractor connection to SIPRNet. For Example:
    a. Computer Network Defense Service Provider (CNDSP) alignment
    b. Host Based Security System (HBSS)
    c. Access to Secure Technical Implementation Guides (STIGs) and other tools (e.g. Assured Compliance Assessment Solution (ACAS))
    d. Contractor email & Domain Name Services (DNS)
    e. SIPRNet Hardware tokens
    f. System access or registration (SGS, PPSM, etc.)
    g. Other requirements as directed by policy

3. Ensure sponsored connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

    - DODI 8510.01, Risk Management Framework (RMF) for DoD IT 24 May 16.
    - DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 18 May 16

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

- DODI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 28 May 14
- CJCSI 6211.02D, DISN: Policy and Responsibilities, dated 24 January 2012
- Network Services Directorate Enterprise Service Division Connection Process Guide; see http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide

4. Facilitate the transition of sponsored connections to a DISA DMZ solution as soon as it becomes available.

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

Disclosure Authorization

NISP contractors are **NOT** permitted unfiltered access to the SIPRNet (CJCSI 6211.02). Sponsor determines access requirements on initial Non-DOD validation letter. If sponsor requires contractor to have additional accesses, the sponsor will be required to fill out a Disclosure Authorization form and submit to disa.scott.conus.mbx.smc-contractor@mail.mil. DISA will update contractor filter for approved access as appropriate.

TASKORDS and Other Directives (Enhanced Controls)

Examples of enhanced controls (not all inclusive; list may be updated as new directives are applicable) are listed below;

Technical:

- DISA Secure Technical Implementation Guides (STIG) used to secure system/networks. For example but not limited to:
  - Network – Enclave, Network Policy, Firewall/IDS, Network Infrastructure
  - Operating System(s) as applicable
  - Host Based Security System
  - Traditional/Physical Security
  - Others as applicable; MS Office, Exchange, Internet Explorer etc.
- HBSS OPORD 12-1016
- DSS CTO 10-133 Removable Media Guidance
- Monthly Vulnerability Scans ACAS (TO 13-0670)
- SIPRNet Hardware Token
  - (TASKORD 12-0863)
- SIPRNet GIAP System (SGS) maintenance (TO 12-1212)

Additional Documentation or Procedural Items:

It is recommended that NISP sites with approved SIPRNet develop and make available Supplemental Operating Procedures to the SSP. The items below are not an all-inclusive list; please refer to applicable STIGs and/or directives for documentable items.

- DoD Warning Banner & IS User Agreements (CTO 08-008A)
  - Acceptable Use Policies (AUP) for both user and privileged user levels
- Insider Threat Mitigation (TASKORD 14-0185)
- Continuity of Operations Plan (COOP)
  - Incident Response Plan

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

  - Disaster Recovery Plan
  - Emergency Destruction Plan
- Configuration/Change Management Plans
  - Configuration Control Board (CCB)
  - Vulnerability Management Program
- Local IA-related policies and procedures, (i.e. firewall maintenance, IDS/audit reviews)
- Appointment letters for security staff members (i.e. System Administrators, ISSM, ISSO)

NISP contractors with connections to government networks as stated above shall coordinate with the sponsor of the network connection to obtain guidance, procedures and any related tools for implementing the enhanced controls required in order to obtain and maintain an accreditation with the DAA of the network. Furthermore, the addition of enhanced controls shall be fully documented in the (M) SSP.

Computer Network Defense Service Provider (CNDSP)

Per CJCSI 6211.02D: Non-DOD ISs connected to the DISN must be covered by accredited CNDS providers IAW DODD O-8530.1. The sponsoring CC/S/A or field activity must ensure that the CNDS provider requirement is defined in a Contract, MOA, or MOU with the non-DOD organization or entity.

Command Cyber Readiness Inspection

In accordance with CJCSI 6211.02D any IS connected to the SIPRNet is subject to Command Cyber Readiness Inspection (CCRI). A certified CCRI team will evaluate enclave and network security, perform network-based vulnerability scans, and assess compliance with applicable policies/CND Directives. Failure to comply with the inspection process or failure to receive a passing score may prompt disconnection of the contractor sponsored SIPRNet connection and require a subsequent re-inspection to ensure compliance. In preparation for a CYBERCOM scheduled compliance inspection it is recommended that sponsors and their contractors conduct self-assessments well in advance. Sponsors are advised to check with their aligned CNDSP for possible pre-CCRI support.

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

SIPRNet GIAP System (SGS) Guidance

A new SGS was deployed on Jan 3, 2013, which requires the customers to upload their Connection Approval Package artifacts and complete the registration for each Mission/Exercise and /or Circuit when requesting an I/ATC.

To gain access to SGS, you must request an account,

1) Go to https://giap.disa.smil.mil/gcap/home.cfm (SIPR)
2) Click "request a SGS account"
3) Upload the completed and signed DD 2875 by clicking the "Browse" Button
4) Click "Submit 2875"
5) Complete the required fields
6) Click "Submit Request"

A DISA analyst will then review your request. You will receive an email message approving or denying your request.

Guidance on uploading SGS documentation for DSS accredited circuits

Note: Complete all required fields of Sections 0-9 of the GIAP Checklist (Sections with a locked icon are reserved for use by CAO Analyst)

***A new connection field, "**Contractor (Non-DoD)",** has been added to the Connection Type drop down in Section 0.1. NISP sites will select "Contractor (Non-DoD)" as the Connection Type. Existing connection shall login to SGS and update their connection type accordingly.

Section 10; each item below requires something in its place (e.g. *.doc)

Scorecard	Upload a blank document titled "Non-DoD connection Not Required"
Detailed Topology	Upload a compete Topology of enclave; Topology will annotate all devices and connections to enclave to include Routers, IA Equipment (firewall/IDSs), Servers/data storage devices etc., and all connections entry/exit points. The diagram will include IP addresses and vendor, model, and software version for all networking

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

	equipment.
SIP	Upload contractor System Security Plan (SSP)
POAM	If applicable upload POA&M
Consent To Monitor	Upload Consent To Monitor with sponsor signature
Statement of Residual Risk	Upload Statement of Residual Risk with contractor management signature
IATO/ATO	Upload DSS accreditation documentation
OSD Approval Memo	Upload current Validation/Re-Validation memo with DISA SSMO signature
GAA	Answer as appropriate
CIO Letter	Upload a blank document titled "Non-DoD connection Not Required"

***Once all fields have a documented uploaded in system a button will appear at bottom of screen to submit to CAO for review.**

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

REFERENCES

Tools and other IA Products:

DISA STIGs (master list)
http://iase.disa.mil/stigs/Pages/index.aspx

STIG Viewer
http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

Security Content Automation Protocol (SCAP) - compliance tool
http://iase.disa.mil/stigs/scap/Pages/index.aspx

DISA HBSS
http://www.disa.mil/cybersecurity/network-defense/hbss (PKI)

Assured Compliance Assessment Solution (ACAS)
https://www.disa.mil/Cybersecurity/Network-Defense/ACAS (PKI)

SIPR Token Guidance
http://iase.disa.mil/pki-pke/Pages/siprnet-pki.aspx (PKI)

DISA Approved Products List (APL)
http://disa.mil/network-services/UCCO (PKI)

National Information Assurance Partnership (NIAP) Common Criteria & Validation Scheme
https://www.niap-ccevs.org/

Information Assurance Vulnerability Management (IAVM) System
https://iavm.csd.disa.mil/

Training

DISA Field Security Operations (FSO) IA Training
https://powhatan.iiie.disa.mil/classroom_training/index.html

DISN Connection Process Training
http://disa.mil/Network-Services/Enterprise-Connections/FAQs/Training-Program-FAQs

Fed Virtual Training Environment (VTE)

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)

NISP SIPRNet Circuit Approval Process
August 2016 v2.4

https://fedvte.usalearning.gov/

POCs and Helpful Links:

Connection Approval FAQ's: http://disa.mil/Services/Network-Services/Enterprise-Connections/FAQs/Connection-Approval-FAQs

DISN Customer Contact Center
disa.scott.conus.mbx.dccc@mail.mil
618-220-9500, option#1 or 800-554-DISN (3476)

DISA SIPRNet Service Manager (SMO)
disa.meade.ns.mbx.classified-connection-approval@mail
1-800-554-DISN (3476)

DISA Classified Connection Approval Office (CAO)
disa.meade.ns.mbx.classified-connection-approval@mail.mil
301-225-2900/2901

DOD NIC (IP registration)
www.nic.mil / www.ssc.smil.mil (SIPR)
800-582-2567

Ports, Protocols, and Services Management (PPSM)
http://disa.mil/Services/Network-Services/Enterprise-Connections/PPSM
(301) 225-2904
dod.ppsm@mail.mil or ppsm@disa.smil.mil (SIPR)

Command Cyber Readiness Inspection (CCRI) Program Information
http://dssinside.dss.mil/ISFO/ODAA/CCRI/default.aspx (PKI)

DISA Web Content Filtering Service (WCFS)
618-220-9129

DSS SIPRNet Program Lead
dss.quantico.dss-hq.mbx.disn@mail.mil

Non-DOD New Connection: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide/Mission-Partner-Connection-Process

Published by Defense Security Service,
National Industrial Security Program Authorization Office (NAO)