SIPRNet Contractor Approval Process (SCAP)
December 2011 v2

Roles and Responsibilities

PARTICIPANT	RESPONSIBILITIES
Defense Security Service (DSS)	• DAA 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. • Signatory authority for IS accreditation decisions, Memorandum of Understanding/Agreements (MOU/A) and SIPRNet Connection Questionnaire (SCQ).
Defense Information Systems Agency (DISA)	• Responsible for Defense Information System Network (DISN) circuits and oversight per CJCSI 6211.02C • Process Connection Approval Packages (CAP) and make connection decisions (IATC/ATC)
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 for contractor connection to SIPRNet (i.e. CNDSP, email, DNS, HBSS)

Published by Defense Security Service,
Office of Designated Approving Authority

SIPRNet Contractor Approval Process (SCAP)
December 2011 v2

Process Overview

Non-DOD Validation of New DISN Connections:

1. Government Sponsor completes and submits the Non-DOD DISN Connection Validation Letter (Validation Letter) to SSMO@disa.mil (download template http://www.disa.mil/connect/library/index.html#csample), contact 1-800-554-DISN (3476). 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 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, DSS, DISA SSMO 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 for the Certification and Accreditation of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM).

    Required documentation to be submitted to DSS ODAA@dss.mil:

    1) The Non-DOD DISN Connection Validation Letter endorsed by the Government Sponsor, the DISA SSMO, and the Service/Agency validation official.
    2) DOD CIO connection approval memo

3) Completed SCQ for Regional Designated Approving Authority (RDAA) signature
4) Consent To Monitor (CTM) memorandum with Government Sponsor's signature.
5) Statement of Residual Risk with contractor signature.
6) SSP and IS Profile
7) Evaluated Assurance Level (EAL) certificates validating at least EAL-4 Firewall and EAL-2 IDS. (http://www.niap-ccevs.org/vpl)
8) Copy of MOU/A or contract signed by CNDSP and sponsor (the MOU/A must be funded/resourced)
9) Risk Acceptance Letter(s) (if applicable)
10) Plan of Action & Milestone(s) (if applicable)

6. Sponsor registers connection information in the SIPRNet IT Registry and requests IP services for the contractor. For more information sponsors shall contact DOD Network Information Center (NIC) at 800-582-2567.

7. Contractor/Sponsor submit Connection Approval Package (CAP) to DISA Classified Connection Approval Office (CAO); CCAO@disa.mil 301-225-2900/2901 and copy DSS at disn@dss.mil. Once package is verified, Interim Authorization to Test (IATT) will be granted by DISA and initiate burn-in testing by DISA Global Network Security Center (GNSC).

Required Documentation to DISA CAO:

1) The Non-DOD DISN Connection Validation Letter endorsed by the Government Sponsor, the DISA SSMO, and the Service/Agency validation official.
2) DOD CIO connection approval memo
3) DSS IATO/ATO letter
4) SCQ w/DSS RDAA signature
5) Consent To Monitor (CTM) memorandum with sponsor signature.
6) Statement of Residual Risk with contractor signature.
7) Network topology diagram.
8) SSP and IS Profile

8. After burn-in and remote compliance vulnerability scan by DISA GNSC, 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).

9. 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. Once system is formally disestablished per the ISFO PM the contractor ISSM shall forward disestablishment letter to CCAO@disa.mil and DISN@dss.mil. 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 with enough time to prevent disconnection because of an expired IATC/ATC (see below).

Non-DOD Revalidation of Existing Connections:

1. Government Sponsor completes and submits the Non-DOD DISN Connection Revalidation Letter to SSMO@disa.mil (download template http://www.disa.mil/connect/library/index.html#csample). Contact 800-554-DISN (3476) or 703-674-5311 for questions.
    - If there is a change in sponsor, mission, requirement, contract or location then DOD CIO approval may be required.

2. DISA Connection Approval Office (CAO) reviews and makes connection decision.

    - DSS oversees recertification and reaccredit as necessary, contractor prepares SSP and required documentation. DSS Certification and Accreditation process is documented in the ISFO PM. ODAA documents can be requested via http://www.dss.mil/isp/odaa/request.html)

    - Prior to DISA CAO granting 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.

Required documentation to be submitted to DSS ODAA@dss.mil:

1) Non-DOD DISN Connection Revalidation Letter endorsed by the Government Sponsor and DISA SSMO

2) SCQ for RDAA signature
3) Consent To Monitor (CTM) memorandum with sponsor signature.
4) Statement of Residual Risk with contractor signature.
5) SSP and IS Profile
6) Evaluated Assurance Level (EAL) certificates validating at least EAL-4 Firewall and EAL-2 IDS. (http://www.niap-ccevs.org/vpl)
7) Copy of MOU/A or contract signed by CNDSP and sponsor (the MOU/A must be funded/resourced)
8) Risk Acceptance Letter(s) (if applicable)
9) Plan of Action & Milestone(s) (if applicable)

3. Contractor/Sponsor submits updated Connection Approval Package (CAP) to DISA Classified Connection Approval Office (CAO) CCAO@disa.mil 301-225-2900/2901 and copy DSS at disn@dss.mil.

Required Updated Documentation to DISA:

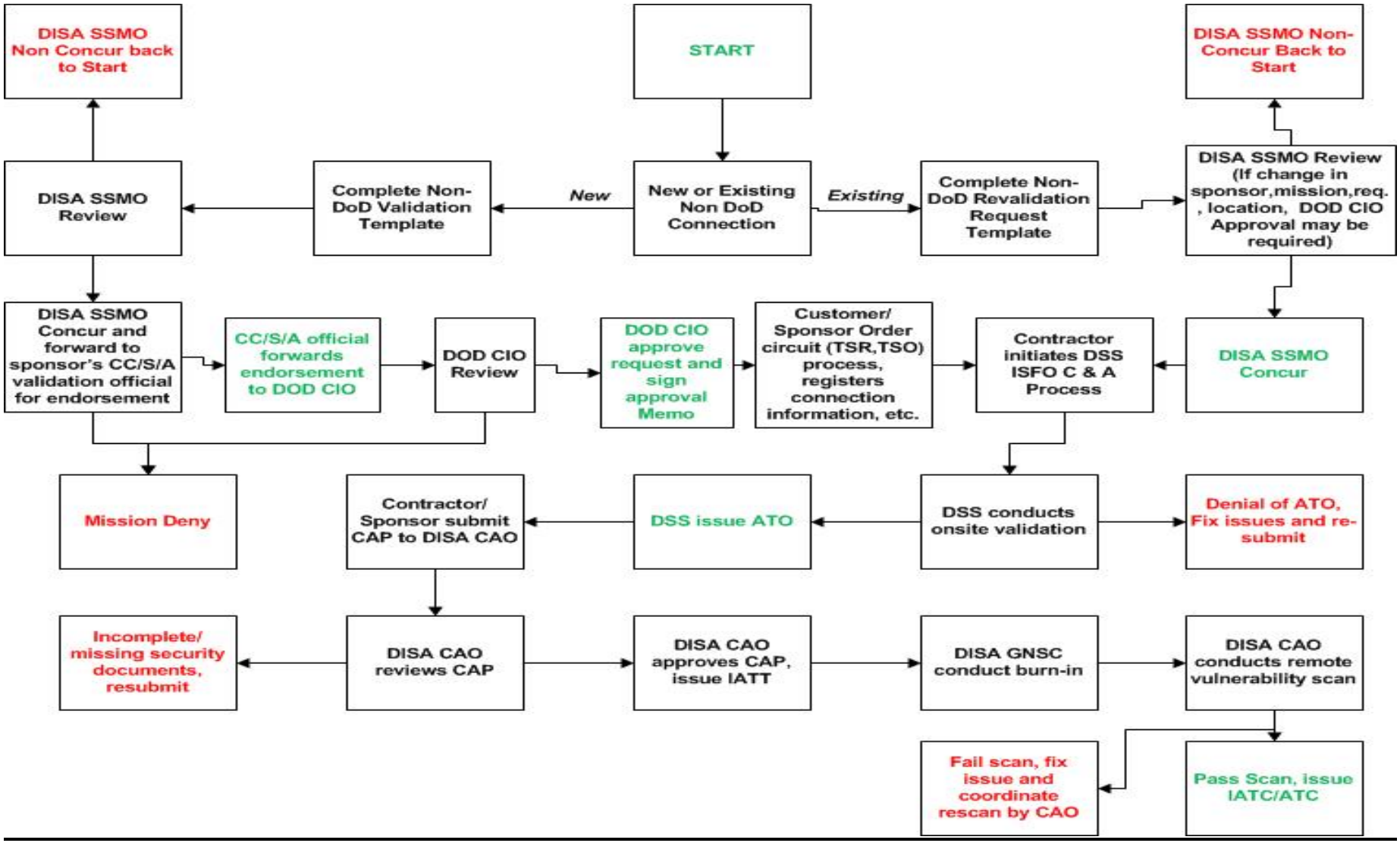
1) Non-DOD DISN Connection Revalidation Letter endorsed by the Government Sponsor and DISA SSMO
2) DSS IATO/ATO letter
3) SCQ w/DSS RDAA signature
4) Consent to Monitor (CTM) memorandum with sponsor signature.
5) Statement of Residual Risk with contractor signature.
6) Network topology diagram.
7) SSP and IS Profile

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

5. 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. Once system is formally disestablished per the ISFO PM the contractor ISSM shall forward disestablishment letter to CCAO@disa.mil and DISN@dss.mil. The sponsor shall then disconnect the service by contacting DISA DDOE.

SIPRNet Contractor Approval Process (SCAP)
December 2011 v2

Process Flow Chart



Published by Defense Security Service,
Office of Designated Approving Authority

SIPRNet Contractor Approval Process (SCAP)
December 2011 v2

Additional Guidance

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 (i.e. CNDSP, email, DNS).

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

    - DODI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process dated 28 Nov 07.

    - DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DOD and contractor information systems dated 28 Feb 06

    - DODI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04

    - CJCSI 6211.02C, DISN: Policy and Responsibilities, dated 9 Jul 08

    - Network Services Directorate Enterprise Service Division Connection Process Guide version 3.2, May 2011

4. Facilitate the transition of sponsored connections to a DISA DMZ solution by October 1, 2012, or as soon as it becomes available.

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 smc-ctr@disa.mil. DISA will update contractor filter for approved access.

Published by Defense Security Service,
Office of Designated Approving Authority

TASKORDS and Other Directives

NISP contractors having Information Systems which connect to DISN SIPRNet may be required to implement enhanced security measures as a result of agreed upon terms in the Approval To Connect (ATC) or the Memorandum of Understanding/Agreement (MOU/A). These systems may be required to implement enhanced security measures beyond the baseline controls in this document as a result of agreed upon terms in the Memorandum of Agreement/Understanding (MOA/U). Failure to implement the additional procedures may add an additional level of risk deemed unacceptable by the DAA of the connected network, resulting in disconnection or denial of an ATC.

A few examples of enhanced controls:

- DSS Communication Tasking Order (CTO) 10-133 Data Transfer Procedures (or other applicable USCYBERCOM Tasking Orders).
- Host Based Security System (HBSS).
- Application of Security Technical Implementation Guides (STIGs), Gold Disk, Retina etc.

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 (i.e. Gold Disk, Retina, and HBSS) required in order to obtain and maintain an ATC 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 6211.02C: 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. For a listing of Non-DOD available CNDSP providers contact SSMO@disa.mil or disn@dss.mil.

SIPRNet Contractor Approval Process (SCAP)
December 2011 v2

REFERENCES

POCs and Helpful Links:

DISN Customer Contact Center
DCCC@csd.disa.mil
800-554-DISN (3476)

DISA SSMO
SSMO@disa.mil or 703-674-5311

DISA CAO
CCAO@disa.mil
301-225-2900/2901

DOD NIC
www.nic.mil / www.ssc.smil.mil
800-582-2567

DISA HBSS
http://www.disa.mil/Services/Information-Assurance/HBSS

DSS SIPRNet PM
disn@dss.mil

DISN Connection Process Links:

Non-DOD New Connection:
http://www.disa.mil/connect/instructions/nonDOD_new_siprnet.html

Non-DOD Existing Connection:
http://www.disa.mil/connect/instructions/nonDOD_exist_siprnet.html

Policy & Process Guides:

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02C, 9 July 2008
DISN Connection Process Guide, for latest version:
http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/Getting-Started/SIPRNET/SIPRNET-NonDOD-New (click download connection process guide)
DODD O-8530.1, 8 January 2001, Computer Network Defense (CND)
DOD 5220.22-M, NISPOM, 28 February 2006
ISFO Process Manual, June 2011 revision 3 (www.dss.mil)

Published by Defense Security Service,
Office of Designated Approving Authority