CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

MEMORANDUM FOR THE DISA CONNECTION APPROVAL OFFICE

SUBJECT: Summary of DoD Sponsor Responsibilities for Mission Partner Connections to the Defense Information Systems Network (DISN)

To achieve and sustain an information advantage, the DoD must be able to securely share information resources with our mission partners to the maximum extent allowed by law and policy. The DoD CIO is authorized to grant mission partners connection to DoD networks when necessary for national security when those activities have critical national security and emergency preparedness needs, and when connection is in the best interest of the U.S. Government.

DoD Components that wish to sponsor mission partner connections to DoD networks are responsible for ensuring the connection is mission essential, properly maintained throughout the connection's lifecycle, and secure. The responsibilities of DoD sponsors are defined in several OSD and Joint Staff issuances and are included in the attached summary with references. DoD sponsors are strongly encouraged to consult the references for additional details.

Request that the DISA Connection Approval Office incorporate the attached summary of DoD sponsor responsibilities into the DISA Connection Process Guide.

The DoD CIO points of contact for this memo are Mr. Thomas N. Orme, 571-372-4431 thomas.orme@osd.mil; and Mr. Leonard Tabacchi, 571-372-4716, leonard.tabacchi.ctr@osd.mil.

ORME.THOMAS.NATHAN.1177093986

Digitally signed by ORME.THOMAS.NATHAN.1177093986
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=ORME.THOMAS.NATHAN.1177093986
Date: 2012.08.14 16:04:12 -04'00'

Thomas N. Orme
Chair, GIG Waiver Panel & Connection Approvals
DOD CIO Governance Directorate

Attachment:
As stated

# Summary of DoD Sponsor Responsibilities for Mission Partner Connections to the Defense Information Systems Network (DISN)

1. DoD components that wish to sponsor mission partner connections to DoD networks are responsible for ensuring the connection is mission essential, properly maintained throughout the connection's lifecycle, and secure. The responsibilities of DoD sponsors are defined in several OSD and Joint Staff issuances and are summarized in this memo with references. DoD sponsors are strongly encouraged to consult the references for additional details.

2. Responsibilities or considerations that affect a DoD Component sponsoring a mission partner (e.g., a DoD Contractor or a non-DoD Federal Department/Agency) connection to DISN include:

a. All connection requests for a mission partner or defense contractor IS to the DISN-provided transport and information services must be endorsed, validated, and submitted by the CC/S/A IAW the DISA Connection Process Guide and the Defense IA Security Accreditation Working Group (DSAWG), DISN/GIG Flag Panel processes. (**reference a**, Enclosure B, paragraph 2.c.(6); **reference b**, sections 5 and 6)).

b. CC/S/As shall maintain oversight for CC/S/A connections and requests, validate operational requirements, and prioritize mission partner and defense contractor connection requests. CC/S/As shall also ensure foreign entity requests are endorsed by a combatant command headquarters. (**reference a**, Enclosure D, paragraphs 2.g.(2) and (3)

c. Facilitate the transition of sponsored mission partner connections to a DISA DMZ solution in accordance with DISA guidance. (**reference a,** Enclosure B, paragraph 2.g, and Enclosure D, paragraph 4.h; **reference i**)

d. Coordinate system(s) provisioning, certification and accreditation (**reference a**, enclosure D, paragraph 7.a; **reference b**, paragraphs 2.1.4, 2.1.6, and sections 5 and 6)

e. Coordinate funding necessary for full implementation (including any future security related POA&M items) of the requested connection per the MOU/MOA, or other official agreement. (**reference a**, Enclosure D, paragraphs 9.e and 9.k; reference **b**, paragraph 2.1.4, and Appendix A line 2.h.)

f. Ensure complete and accurate information about mission partner system/network operated on behalf of the DoD are registered in the appropriate databases (**reference a**, Enclosure B, paragraphs 1.c.(2).(c), 2.b.(2), 2.c.(3), and 2.d; **reference b**, paragraph 3.4, 5.8, and Appendix D, paragraph D.2.)

(1) Unclassified DoD IT Program Registry (DITPR) (https://ditpr.dod.mil),
(2) Classified SIPRNet IT Registry:

- To request an account and access to the application: https://arm.osd.smil.mil
- Once you have an account the SIPRNet link is: http://dodcio.osd.smil.mil/itregistry

(3) Unclassified IP Address ranges - Network Information Center (https://www.nic.mil),

(4) Classified IP Address ranges - SIPRNet Support Center (www.ssc.smil.mil)

(5) Unclassified Circuits - SNAP (https://snap.dod.mil)

(6) Classified Circuits - GIAP/SGS (https://giap.disa.smil.mil)

(7) Ports, Protocols, and Services Management (PPSM) (https://pnp.cert.smil.mil) on SIPRNet for all networks/systems ports, protocols, and services for all IP solutions or applications

(8) Vulnerability Management System (VMS)

- To request an account contact – DISA at 405.739.5600 opt 4
- Once you have an account, VMS can be accessed at https://vms.disa.mil   or https://vms.disa.smil.mil)

(9) Voice soft switches connected to the DISN shall be registered in SNAP DSN and obtain connection approval. (i.e., LSC, MFSS, WANSS)

g. Ensure requirement for alignment with an accredited Computer Network Defense Service Provider (CNDSP) is defined in a contract, MOA or MOU and funded  (**reference a,** Enclosure B, paragraph 5.b, and Enclosure D, paragraphs 2.d, 9.e, and 9.i;  **reference b**, paragraph 2.1.2, and Appendix A line 2.d;  **reference c**, paragraphs 4.1 and 4.5; **reference d**, paragraph 5.5.7;  **reference e**, enclosure C, paragraph 3.c.(2))

h. Ensure the DAA notifies DISA and DoD CIO of all renewals and modifications to approved renewal requests for mission partner or defense contractor connection or if there is a significant change in the original operational requirements (e.g. mission, architecture, supporting contractor) for which the approval was granted.  (**reference a**, Enclosure D, paragraph 9.n;  **reference b**, paragraphs 3.7.1, 4.1, 4.6.1, 5.11.1, 6.1, 6.6.1, Appendix A (see first note), and Appendix B, 2nd paragraph)

i. Ensure that DOD, mission partner, or defense contractor ISs connected to DISN-provided transport and information services are authorized to operate IAW DOD, IC, or other governing policy and processes.  (**reference a**, Enclosure D, paragraph 2.b)

j. Provide security control assessment (certification) and authorization to operate (accreditation) documentation IAW DODI 8510.01 (**reference f**), ICD 503  (**reference k**), or NIST SP 800-37 (**reference l**) as appropriate for deploying IS to receiving CC/S/As. For defense contractor classified ISs, DOD 5220.22- M (**reference g**) documentation will be provided.  (**reference a**, Enclosure D, paragraph 2.b (see footnote 21))

k. Ensure at least annually that ISs are reviewed for compliance with DOD IA requirements, including mission partner and defense contractor ISs sponsored by the CC/S/A. (**reference a**, Enclosure D, paragraphs 2.k, and 9.j.(3);  **reference e**, Enclosure C, paragraphs 6.f.(4), 6.j.(2), 6.j.(3), and 20.)

l. Ensure mission partners are advised of and acknowledge through formal agreements (e.g., contract, MOA, or MOU) the conditions for connection to DISN-provided transport and information services. (**reference a**, Enclosure D, paragraph 9.k; **reference b**, Sections 5 and 6.)

m. Providing an unauthorized DISN connection to a mission partner or defense contract and unsatisfactory inspection results are grounds for potential immediate disconnection of the CC/S/A connection to DISN-provided transport and information services. (**reference a**, Enclosure B, paragraph 7.a, and Enclosure D, paragraph 14.b.(2).(c))

n. Ensure (and report) proper disconnection of non-DoD entities immediately upon mission termination or change of contract/MOU/MOA - submit a “discontinue” request through the DISA Direct Order Entry Process (**reference a**, Enclosure D, paragraph 3.d; **reference b**, paragraph 2.1.4)

3. References

a) CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities, 24 January 2012
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf

b) DISA Connection Process Guide (CPG), June 2012
http://www.disa.mil/connect/ (interactive website)

c) DoDD O-8530.1 Computer Network Defense (CND), January 8, 2001
http://www.dtic.mil/whs/directives/corres/pdf/O85301p_placeholder.pdf

d) DoDI O-8530.02, Support to Computer Network Defense (CND), March 9, 2001
http://www.dtic.mil/whs/directives/corres/pdf/O85302p_placeholder.pdf

e) CJCSI 6510.01F, Information Assurance (IA) and Computer Network Defense (CND), 9 February 2011
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

f) DoDI 8510.01 , Department of Defense Information Assurance Certification and Accreditation Process, November 28, 2007
http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf

g) DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 28, 2006
http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf

h) DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), August 13, 2004
http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf

i) OSD Connection Approval Memorandum issued by DoD CIO for each mission partner connection.

j) DoDD 8000.01, Management of the Department of Defense Information Enterprise, February 10, 2009
http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

k) Intelligence Community Directive Number 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008

l) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf