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

CHIEF INFORMATION OFFICER

NOV 2 2 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR OF THE DOD FIELD ACTIVIES

SUBJECT: Interim Guidance on Networthiness of Information Technology (IT) Connected to DoD Networks

Networthiness is the result of an operational assessment of IT to verify compliance with security, interoperability, supportability, sustainability, and usability regulations; guidelines, and policies as issued by Federal, DoD, and Combatant Command/Service/Agency Components. This memorandum promulgates a standard set of Networthiness criteria as interim guidance to establish consistent policies and procedures across DoD Components and to achieve efficiencies by eliminating redundant requirements for IT assessments and certifications. It facilitates reciprocity, decreasing the time needed for the cross-Component fielding of IT. The Networthiness criteria will be incorporated into the DoD Instruction.

DoD Components should begin to incorporate this guidance into their existing IT certification processes in preparation for a forthcoming DoD Instruction, which will further refine and codify this memorandum. The point of contact for this matter is Mr. Tom Lam at email: thomas.lam@osd.mil, 571-372-4686.

Teresa M. Takai

Attachments:
1. References
2. Networthiness Criteria

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005

(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009

(c) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008

(d) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002

(e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

(f) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007

(g) Directive Type Memorandum 08-027, "Directive-Type Memorandum (DTM) 08-027 – Security of Unclassified DoD Information on Non-DoD Information Systems," September 16, 2010

(h) DoD Principal Accrediting Authorities Memorandum, "Information System Certification and Accreditation Reciprocity," July 23, 2009

(i) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004

(j) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004

(k) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," June 30, 2004

(l) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010

(m) Chairman of the Joint Chiefs of Staff Instruction 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," December 15, 2008

(n) DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008

(o) DoD CIO Executive Board Charter, July 7, 2005

NETWORTHINESS CRITERIA

1. GENERAL. Networthiness is the result of an operational assessment of IT to verify compliance with security, interoperability, supportability, sustainability, and usability regulations, guidelines, and policies as issued by Federal, DoD, and Combatant Command/ Service/Agency Components. Consistent Networthiness assessment of IT connecting to DoD networks across DoD Components improves security and interoperability, facilitates reciprocity, and reduces the time needed for the cross-Component fielding of IT. This attachment identifies a baseline set of standard Networthiness criteria to be used in assessing IT connecting to DoD networks. The DoD CIO, in coordination with the DoD Components, will maintain an official version of these criteria per authorities established in References (a) and (b). The official online version will be available on the DISA Unified Capabilities Certification Office (UCCO) homepage at http://www.disa.mil/ucco/.

a. Criteria and Descriptions. Table 1 identifies a list of criteria, a description of each set of criteria, and the associated data requirements for Networthiness assessments. In some cases, the data requirements will be met by an existing artifact. As such, the Data Requirements /Artifacts column includes recommended artifacts that satisfy a subset of the data requirements for each set of criteria. Recommended artifacts are not all inclusive. For security, required artifacts are specified as these are mandated by existing policy. DoD Components responsible for deploying the IT and for subsequently, obtaining a Certificate of Networthiness (CoN - determination by a DoD Component that a system, application, or product meets Networthiness criteria) should leverage existing artifacts from other processes and reporting requirements to meet the data requirements of Networthiness. DoD Components responsible for issuing a CoN should accept for review existing artifacts and supporting documents from other assessments/ certifications to satisfy CoN data requirements.

Table 1. Networthiness Criteria

Criteria	Description (The IT...)	Data Requirements/Artifacts
Acquisition Guidelines and Usability	Meets design specifications, complies with architecture, and is successfully tested and accepted by the user.	**Data Requirements** • List of technical standards employed • Evidence of user acceptance • Evidence of Central Contractor Registration (CCR) of all vendor manufacturers • Compliance with DoD enterprise architecture • Compliance with Clinger Cohen Act **Recommended Artifacts** • Standards Profile (e.g., StdV-1) • Formal user acceptance memorandum • CCR number(s) • Relevant artifacts from DoD Information Enterprise Architecture, Appendix G • Relevant artifacts from DoDI 5000.02

		(Reference (c)), Enclosure 5, Table 8
Security	Meets all security-related criteria as defined by References (d), (e), (f), (g), (h), and DoDI 8551.1 (Reference (i)).	**Data Requirements** • Evidence of security criteria compliance • Identification of ports, protocols, and services • Identification of Computer Network Defense Service Provider **Required Artifacts** • DIACAP Package • Authorization to Operate (ATO) • List of ports, protocols, and services • Designation of Computer Network Defense Service • Provider in writing
Interoperability	Meets all interoperability and supportability requirements as identified in References (j), (k), (l), and (m).	**Data Requirements** • Compliance with NR-KPP (includes data flow descriptions and evidence of IPv6 compatibility) • Evidence of meeting interoperability criteria **Recommended Artifacts** • Information Support Plans • Joint Interoperability Test Center (JITC) Interoperability Certification • Joint Staff (JS) Interoperability & Supportability (I&S) Certificate • UC Approved Products List (APL) or Unified Capabilities Requirements (UCR) Standards verification • IPv6 Compliance Verification
Supportability and Sustainability	Is sufficiently supported throughout its lifecycle to ensure continuous operation and maintenance.	**Data Requirements** • Evidence that a resource support plan is in place to include documentation of a dedicated funding stream (e.g., program execution lines) • Documented installation information to include facilities requirements (e.g., electricity, HVAC, space dimensions, power outage plans) • Documented implementation and transition plans • Documented configuration management plans • Evidence that a training plan is in place for users and support personnel to include documentation of help desk availability

		Recommended Artifacts • Service Level Agreements • Information Support Plans • JS I&S Certificate
Network Utilization	Sufficiently supplies information regarding network utilization to enable determination of network impact (e.g., performance, security, and configuration impacts).	**Data Requirements** • Radio frequency • Spectrum registration • Information on wireless capability to include RADIUS server access control implementation, a FIPS 140-2 certificate, proof of "802.1x with EAP-TLS mutual authentication" compliance, a Wi-Fi Alliance Certification, and HERO/HERP testing results (if applicable) • Bandwidth utilization to include location of where IT will be hosted, location of where IT will be used, description of user capacity schedule (peak usage times), and estimated bandwidth usage for both in-band & out-of-band use (if applicable) • SATCOM requirements to include where in the network segment the satellite resides, satellite ownership (e.g., commercial, DoD-owned, DoD-leased), band usage (e.g., wide, narrow, protected), and description of channel allocation **Recommended Artifacts** • DD Form 1494 • Spectrum registration number • JS I&S Certificate
DoD Policy Compliance	Supplies all policy waivers as granted by a formal governance body (e.g., if using a non-DoD standard collaboration tool, must supply a DoD Enterprise Services Collaboration Capabilities Waiver issued by the GIG Waiver Panel).	**Data Requirements** • Information on waivers **Recommended Artifacts** • Formal waiver memorandum

b. IT Categories. Table 2 identifies the criteria exceptions associated with each IT category, which includes systems, applications, and products. IT that qualifies as a NetOps or IA capability may require additional criteria in compliance with DoDI 8410.02 (Reference (n)) and References (d), (e), (f), (g), and (h).

Table 2. Criteria Exceptions by IT Category

Criteria	Systems	Applications	Products
Acquisition Guidelines and Usability	• Clinger Cohen Act Compliance not required for non-ACAT systems	• Clinger Cohen Act Compliance not required for IT purchases under three thousand dollars • Web services require only information sharing agreements between participating parties	• DoD enterprise architecture compliance not required • Compliance with local architectures is required • Clinger Cohen Act Compliance not required for IT purchases under three thousand dollars • Products in DoD-recognized Approved Product Lists fulfill requirements
Security	• No exceptions	• No exceptions	• Computer Network Defense Service Provider not required for products
Interoperability	• No exceptions	• No exceptions	• No exceptions
Supportability and Sustainability	• No exceptions	• Facility requirements not required	• No exceptions
Network Utilization	• No exceptions	• SATCOM requirements not required	• SATCOM requirements not required
DoD Policy Compliance	• No exceptions	• No exceptions	• No exceptions

PROCEDURES

1. GENERAL. A CoN is a determination by a DoD Component that a system, application, or product meets Networthiness criteria. This attachment provides guidelines for implementing a CoN process. It includes procedural guidance for resolving issues concerning CoN approval decisions and for submitting change recommendations to Networthiness criteria.

2. GOVERNANCE. The DoD CIO will designate a subordinate body under the DoD CIO Executive Board (Reference (o)) as the Networthiness Steering Group to coordinate policy and to provide oversight and direction across DoD Components in support of Networthiness implementation. The DoD CIO Executive Board will function as the key advisor and arbitrator for all Networthiness issues on behalf of the DoD CIO. For those issues which impact security, the DoD CIO Executive Board will coordinate with the Defense Information Assurance Security Accreditation Working Group (DSAWG), the Defense Information Systems Network (DISN)/ GIG Flag Panel, and the DoD PAAs as appropriate.

Table 3. Networthiness Governance Body Roles and Responsibilities

Governance Body	Roles and Responsibilities
DoD CIO Executive Board	• Reviews issues that cannot be resolved among DoD Components • Provides DoD CIO with recommendations concerning issue resolution
Networthiness Steering Group as designated by the DoD CIO	• Proposes, reviews, updates, and coordinates Networthiness policy, criteria, and requirements • Reviews disputed CoNs • Reviews critical Networthiness issues and defines associated strategies for addressing issues • Escalates issues to the DoD CIO Executive Board that cannot be resolved at this level

3. IMPLEMENTATION GUIDELINES. The Heads of the DoD Components should implement a CoN process for the portions of the Defense Information Enterprise within their assigned AOR. CoN processes should include registration of issued CoNs in an enterprise-level repository, which federates to a DoD enterprise-level repository as maintained by DISA.

a. CoN-Issuing Organization.

(1) The Head of a DoD Component should identify an organization responsible for assessing and issuing CoNs. DoD Components deploying IT should apply for a CoN through this organization. This organization should uniquely identify the CoN application using an authoritative identifier (e.g., DITPR, eMASS) when possible and must be resourced to analyze CoN applications in a timely manner as determined by operational requirement. They should electronically capture CoN artifacts in a central repository with visibility and accessibility to all authorized users. They should also define and publish the test measures used to determine if the CoN application satisfies each Networthiness criterion.

b. CoN Approval.

(1) Prior to approval, the CoN-issuing organization should review the CoN application for completeness and validate that it meets the standard Networthiness criteria. By issuing a CoN, the CoN signature authority certifies that the IT meets the standard Networthiness criteria identified herein. Upon approval, the CoN-issuing organization should register the CoN in an enterprise-level repository, which should federate to a DoD enterprise-level repository. Certificates registered in a DoD enterprise-level repository should be recognized and leveraged by DoD Components across the DoD Information Enterprise for network enclaves comparable to the network enclave addressed in the original assessment. The CoN-issuing organization should ensure that any change to the status of a CoN is reflected in the DoD enterprise-level repository.

(2) CoN approval may be integrated into existing processes or may be incorporated into other certificates or documents.

c. Reciprocity.

(1) The CoN process should facilitate two levels of reciprocity: mutual agreement among participating enterprises to accept one another's Networthiness assessments and enterprise-level recognition of a CoN. Enterprise recognition in this context means that the CoN data is accurate based on the original assessment and may be leveraged or reused to support assessments by other DoD Components.

(2) The DoD Component deploying the IT should apply for a CoN through a CoN-issuing organization. To meet the standard Networthiness requirements, the DoD Component deploying the IT should engage the DoD Component(s) responsible for the DoD or Service network enclave where connection will occur in preparing a CoN application for the first time. This ensures that the IT complies with the functional requirements, performance objectives, and technical specifications of the network enclave. Early engagement between participating enterprises can facilitate mutual agreement to accept one another's assessments.

(3) Registering issued CoNs in a DoD or Service enterprise-level repository constitutes formal recognition by DoD. Recognition by DoD certifies that the CoN data is accurate based on the original assessment and that it may be leveraged or reused to support assessments by other DoD Components for comparable network enclaves. DoD Components responsible for network enclaves maintain the right to review enterprise-level CoNs; however, should they not recognize the CoN, they should provide a rationale to the DoD CIO for consideration and review. Non-recognition indicates that the CoN data is inaccurate based on the original assessment. The DoD CIO will maintain the right to review any CoNs registered in a DoD or Service enterprise-level repository.

4. PROCESS VALIDATION. The DoD CIO will validate CoN processes employed across the DoD Information Enterprise to ensure that they are consistently assessing IT against standard Networthiness criteria. The DoD CIO will maintain a published list of validated process owners to promote the sharing of best practices, collaboration among Neworthiness reviewers, and cross utilization of processes to maximize productivity.

5. ISSUE RESOLUTION. At any time, a DoD Component may request that the Networthiness Steering Group review the validity of a CoN process, an issued CoN, or a non-issued CoN decision. The DoD Component should submit the issue along with any supporting information to the Networthiness Steering Group. The Networthiness Steering Group will review the information and present a strategy for resolution. If the DoD CIO Executive Board accepts the Networthiness Steering Group recommendation, the affected organizations will be notified with an opportunity to respond within an allotted timeframe. If no critical objections are presented within that timeframe, the recommendation will be implemented. If objections arise and the DoD CIO Executive Board cannot come to any resolution, the issue will be brought before the DoD CIO for final decision.

6. NETWORTHINESS CRITERIA CHANGE REQUESTS. The Networthiness Steering Group will update Networthiness criteria in coordination with the DoD Components. They will establish a change request process and a specified timeframe for reviewing and approving requests.