Department of Defense

INSTRUCTION

NUMBER O-3600.03
April 22, 2010
Incorporating Change 1, November 19, 2010

USD(I)

SUBJECT: Technical Assurance Standard (TAS) for Computer Network Attack (CNA) Capabilities

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) O-3600.3 (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5143.01 (Reference (b)).

b. Updates policies and responsibilities for the TAS for CNA capabilities (hereafter referred to as the "CNA TAS") pursuant to Reference (b).

c. Implements DoDD 3600.01 and Secretary of Defense roadmap (References (c) and (d)) by establishing policy and guidance for development, implementation, and maintenance of the CNA TAS.

(b)(3):10 USC § 130 [redacted]

2. APPLICABILITY. This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

(b)(3):10 USC § 130

e. CNA capabilities shall be classified in accordance with DoDI O-3600.02 (Reference (g)).

(b)(3):10 USC § 130

g. TAS evaluations shall not be conducted on the Global Information Grid.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3 for the structure and role of the IO and Space EXCOM, and Enclosure 4 for procedures for developing the CNA TAS.

7. INFORMATION REQUIREMENTS. The reporting requirements in this Instruction are exempt from licensing in accordance with paragraphs C4.4.1., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (h)).

8. RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. ~~Authorized users may obtain copies on the SECRET Internet Protocol Router Network from the DoD Issuances Website at http://www.dtic.smil.mil/whs/directives~~ *It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.*

9. EFFECTIVE DATE. This Instruction is effective immediately.

James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. IO and Space EXCOM
4. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive O-3600.3, "Technical Assurance Standard for Computer Network Attack (CNA) Capabilities," May 13, 2005 (hereby cancelled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(c) DoD Directive 3600.01, "Information Operations (IO)," August 14, 2006
(d) Secretary of Defense, "Information Operations Roadmap," October 30, 2003[1]
(e) Under Secretary of Defense for Intelligence Memorandum, "Information Operations (IO) and Space Executive Committee (EXCOM) Charter," January 11, 2005[2]
(f) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008
(g) DoD Instruction O-3600.02, "Information Operations (IO) Security Classification Guidance," November 28, 2005
(h) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998

[1] Available at http://webhost.policy.osd.pentagon.smil.mil/ioroadmap.

[2] Available at https://esnet.itiss.osd.smil.mil/iodirectorate. (Enter website as "View Site as Guest.")

ENCLOSURE 2

RESPONSIBILITIES

1. USD(I). The USD(I), pursuant to References (b), (c), and (e), shall:

a. Provide policy for the effective development, implementation, and maintenance of the DoD CNA TAS.

b. Coordinate all CNA TAS activities across the Department of Defense.

(b)(3):10 USC § 130

d. Coordinate with the Heads of the DoD Components that develop or sponsor CNA capabilities to designate an organization within their Component to be the Component's authoritative, single point of contact for the CNA TAS evaluation policies and procedures, evaluation results, and evaluation documentation.

e. Coordinate with the Heads of the DoD Components that develop or sponsor CNA capabilities to designate an organization within their Components to provide the program management office responsibilities of preparing, coordinating, integrating, and sustaining viable CNA capabilities for operational use.

2. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) shall:

a. Identify and support investments in technologies that enable TAS evaluations to verify fulfillment of current and future DoD requirements.

b. Promote joint and cooperative research, development, acquisition, and application of assurance evaluation technologies and processes among the DoD Components.

c. In coordination with the USD(I), implement the CNA TAS consistently within testing and evaluation and IO range environments.

d. In coordination with the DoD Components and as a member of the IO and Space EXCOM, recommend to the USD(I) updates and revisions to the CNA TAS to maintain consistency in evaluations across the Department of Defense.

3. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Incorporate TAS evaluations into the development and life-cycle management processes of their Component CNA capabilities.

b. Provide a representative from their Component to the IO and Space EXCOM to advise the USD(I) on CNA TAS matters.

c. Coordinate with the USD(I) to designate an office of primary responsibility within their Component to communicate with the IO and Space EXCOM on technical issues related to the TAS.

d. Coordinate with the USD(I) to designate an organization within their Component to provide the program management office responsibilities of preparing, coordinating, integrating, and sustaining viable CNA capabilities for operational use if their Component develops or sponsors CNA capabilities.

(b)(3) 10 USC § 130

(1) Using a Component-designated independent organization to conduct TAS evaluations of CNA capabilities in accordance with the CNA TAS and this Instruction.

(2) Designating an authoritative single point of contact for the CNA TAS and TAS evaluation policies and procedures, results, and documentation.

(3) Directing CNA capability developers to capture best practices for TAS evaluations and to propose modifications to the CNA TAS to the Component IO and Space EXCOM representative for consideration by the IO and Space EXCOM.

(4) Documenting and making available to the Combatant Commanders and the IO and Space EXCOM the results of TAS evaluations.

(b)(3) 10 USC § 130

5. COMMANDER, UNITED STATES JOINT FORCES COMMAND (CDRUSJFCOM). The CDRUSJFCOM, through the Chairman of the Joint Chiefs of Staff, shall, in addition to the responsibilities in sections 3 and 4 of this enclosure, provide support to DoD Components conducting TAS evaluations upon the request of the individual Component.

(b)(3):10 USC § 130

[redacted]

(b)(3):10 USC § 130

[redacted]

ENCLOSURE 4

PROCEDURES

1. CNA TAS PURPOSE. The purpose of the CNA TAS is to:

a. Improve the consistency of TAS evaluations.

b. Optimize the planning and execution of required developmental and operational evaluations.

c. Provide the task objectives set forth in the appendix to this enclosure that the DoD Components must accomplish to meet each of the ELAs as defined in the Glossary.

(b)(3):10 USC § 130

[redacted]

3. CNA TAS APPLICATION. The DoD Components shall complete TAS evaluations:

a. Between DTE and fielding of CNA capabilities.

b. For existing CNA capabilities once placed in an operational status. Data captured during operational testing and employment may be used as input to the evaluation.

c. Whether the CNA capability is a single capability or a system of capabilities. If the capability or any of its components is modified after the TAS evaluation, the capability shall be re-evaluated.

d. Prior to employment of capabilities obtained from sources outside the Department of Defense.

(b)(3):10 USC § 130

[redacted]

5. EXCEPTIONS TO POLICY

(b)(3):10 USC § 130

[redacted]

Appendix
Required Task Objectives for ELAs

APPENDIX TO ENCLOSURE 4

REQUIRED TASK OBJECTIVES FOR ELAs

1. INTRODUCTION. This appendix provides a description of the CNA TAS ELAs and the specific task objectives required to achieve each ELA for CNA capabilities. The DoD Components are responsible for establishing procedures to satisfy these objectives.

(b)(3):10 USC § 130

[redacted]

3. TASK OBJECTIVES

(b)(3):10 USC § 130

[redacted]

(b)(3) 10 USC § 130

[redacted]

(b)(3) 10 USC § 130

[redacted]

(b)(3):10 USC § 130

[redacted]

GLOSSARY

PART I. ACRONYMS

CDRUSJFCOM	Commander, United States Joint Forces Command
CIOF	capability IO functions
CM	configuration management
CNA	computer network attack
CRS	capability requirements specification
DoDD	DoD Directive
DoDI	DoD Instruction
DTE	developmental test and evaluation
ELA	evaluated level of assurance
EXCOM	executive committee
IO	information operations
IT	information technology
OT&E	operational test and evaluation
SES	senior executive service
TAS	technical assurance standard
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this Instruction.

adverse illumination. The documented analysis of unintentional capability influence on the environment that may draw undesired attention to the capability, or that may unintentionally and noticeably interfere with proper and expected behavior of the environment.

attribution. The documented analysis of the potential to identify the source, purpose, and/or originator of a capability and/or action either concretely or through plausible inference inherent in a capability and the data generated by the capability.

capability summary specification. A description of how a capability meets the identified IO requirements.

(b)(3):10 USC § 130 [redacted]

characterization. The documented analysis of relevant features, traits, qualities, and properties of a capability that yields observations but not a verdict.

CIOF. The set of all hardware, software, firmware, techniques, and concepts of a capability that must be relied upon for the correct implementation of the capability IO requirements.

CIOF internals. The design structure of the CIOF supporting modularity and minimizing the complexity of functions.

CM automation. The automated functions of a CM system that control modifications to the configuration items of a capability.

CM capabilities. The features and functions of a CM system that ensure a capability is correct and complete; ensure that no configuration items are missed during evaluation; and prevent unauthorized modifications, additions, or deletions to the capability.

CM scope. A list of capability configuration items that need to be placed under CM control.

CNA capability. Any CNA device, weapon, computer program, or technique developed to attack computer networks.

conditional. The description of assurance requirements for a task objective activity that may not be required depending on the IO functional requirements of the capability.

conformance claim. A statement that identifies a source of requirements met by a capability and the CRS.

co-optability. The documented analysis of the potential for a capability or aspects of a capability to be recruited, used, or reused without authorization, and the estimated level of effort required to recruit, use, or reuse a capability without authorization.

coverage. Evidence to show that IO functions described in the functional specification are tested.

covert channel analysis. The documented analysis of a capability's exploitable signaling channels that may exist during capability operations and that may be exploited by an adversary.

CRS. The documented description of the IO requirements implemented by a CNA capability. The CRS identifies how the IO requirements implemented in the capability are derived from the IO technical objectives for the capability and the capability's IO environment.

de-installation. Procedures necessary to properly remove a capability from its operational environment.

depth. The documented analysis of the correspondence between tests identified in the functional test documentation and the internal structure of a capability as defined by the high-level design.

detectability. The documented analysis of the ability of a capability and the data it generates to elude discovery or suspicion of existence, actively and/or passively.

development security. Documentation that describes the physical, procedural, personnel, and other counterintelligence and security measures used in the development environment.

(b)(3):10 USC § 130

[redacted]

employment. The strategic, operational, or tactical use of forces, weapon systems, or other assets.

environmental dependencies. Tests for a capability's environmental interactions, its reactions to unexpected environmental circumstances (conflicts), and its ability to recover and continue operations in the face of unexpected circumstances.

(b)(3):10 USC § 130

[redacted]

functional specification. Description of capability IO functions and user-visible interfaces.

functional test documentation. Documentation consisting of a test plan, test procedures, expected results, and actual results to demonstrate functional testing of a capability.

Global Information Grid. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The global information grid (GIG) includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG information technology (IT) includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

high-level design. A description of a capability's subsystems, identifying the functions they provide.

implementation representation. The documented analysis of the lowest level of detailed internal workings (e.g., source code) of a capability.

independent testing. Tests showing that a capability's IO functions perform as specified and are documented by a designated TAS evaluation organization.

installation, generation, and start-up. The procedures necessary to ensure proper installation, generation, and start-up of a capability.

introduction. A description of a capability in a narrative way that identifies the labeling information necessary to control the CRS and capability, identifies the capability's intended usage and type, and describes the capability's logical and physical scope and boundaries.

IO environment. A detailed description of the environment in which a capability is intended to be used. It identifies all environmental assumptions and expectations and any targeted vulnerabilities, IO mission directives, and threats countered by the capability.

IO requirements. IO functional and assurance requirements, claimed to be implemented by a capability, that enable the capability to meet its IO technical objectives.

IO technical objective modeling. The precise presentation of the important aspects of a capability's IO technical objectives and their relationship to the behavior of the capability. The IO technical objective model describes the rules and characteristics of the IO technical objectives that can be modeled.

IO technical objectives. Moderately detailed descriptions of the technical means by which a capability will exploit targeted vulnerabilities, counter identified threats to the capability, and implement identified IO mission directives, within environmental assumptions and expectations.

life-cycle definition. Documentation that describes the life-cycle model used to develop and maintain a capability.

limited probability of detection. The documented analysis of calculated detectability risks of using a capability.

low-level design. A description of the internal workings of a capability in terms of modules, identifying the functions they provide.

performance. A test of the compliance of a capability, system, or component against specified performance requirements.

policy, law, and regulation. The documented analysis of the use of a capability that could violate policies, laws, and regulations.

post-evaluation deficiency remediation. The procedures used to track and correct flaws discovered by capability users while the capability is supported by the developer.

representation correspondence. The documented analysis of correspondence between the development documentation and a capability summary specification.

security vulnerability analysis. The documented analysis of a capability's exploitable counterintelligence/security weaknesses that could render the capability unable to achieve its required effect.

systematic. Orderly, planned, and methodical performance of the specified analysis or activity.

task objective activities. A second hierarchical level of assurance requirement grouping, each containing like-kind technical objectives of increasing levels of rigor, depth, and scope.

task objectives. The highest hierarchical levels of assurance requirement grouping, each containing activities that share a common focus.

technical assurance. The evaluated basis for confidence that a CNA capability will meet its technical objectives.

tools and techniques. The documented analysis of the security risks of the tools used to develop, analyze, and implement a capability.

user document(s). Instructions and guidelines for the proper use of a capability.