CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-6 CJCSM 6510.03
DISTRIBUTION: A, B, C 28 February 2013

DEPARTMENT OF DEFENSE CYBER RED TEAM CERTIFICATION AND ACCREDITATION

Reference(s): Enclosure F.

1. Purpose

a. This manual, in accordance with references a through k, provides guidance for certifying and accrediting DoD Cyber Red Teams with the ability to evaluate Computer Network Defense Service Providers (CNDSPs) and/or prior to live play on DoD networks. It describes evaluation preparation, grading criteria, processes, and procedure for the certification and accreditation (C&A) process. **Note**: The entire team is certified and accredited versus individuals of a team. Additionally, the C&A process identified within this manual should not be confused with the DoD Information Assurance Certification and Accreditation Process, which is used to accredit DoD information systems.

b. For the purpose of this manual, "Red Team" refers to a DoD Cyber Red Team that possesses a current accreditation, and the organization requesting a C&A evaluation is referred to as the "applicant." The term "C&A evaluation team" or "evaluation team" refers to the National Security Agency (NSA)-led group conducting the evaluation.

c. Deviations from the requirements identified in this manual must be coordinated through the Certification Authority (CA) and approved by the Accreditation Authority (AA).

2. Cancellation. None.

3. Applicability. This manual applies to the Joint Staff, Combatant Commands, Services, Defense Agencies, and Department of Defense (DoD) field and joint activities (hereafter referred to as CC/S/As).

4. Procedures. See Enclosures B through E.

5. Releasability. This manual is approved for public release; distribution is unlimited. DoD components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this instruction/ manual/notice through the Internet from the Chairman of the Joint Chiefs of Staff (CJCS) Directives Home Page--http://www.dtic.mil/cjcs_directives.

6. Effective Date. This manual is effective upon receipt.

CURTIS M. SCAPARROTTI
Lieutenant General, U.S. Army
Director, Joint Staff

Enclosure(s):

A – DoD Cyber Red Team Definition and Overview
B – Phase I - Registration
C – Phase II - Verification
D – Phase III - Validation
E – Phase IV – Post Accreditation
F – References
GL - Glossary

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

DOD CYBER RED TEAM OVERVIEW

1. CYBER RED TEAM DEFINITION AND OVERVIEW

A DoD Cyber Red Team is a group of DoD personnel (military, civilian, contractor) authorized and organized to emulate a potential adversary's exploitation or attack capabilities against a targeted mission or capability. DoD Cyber Red Teams operate to identify exposed information and vulnerabilities of the target's security posture; support information assurance readiness; create a degraded, disrupted, or denied cyber environment; develop the skills and exercise capabilities of cyber forces; participate in evaluation of Computer Network Defense Service Providers (CNDSPs) and its subscribers; and provide Protect Services for CNDSPs or support OPSEC surveys. A DoD Cyber Red Team achieves its purpose by conducting cyberspace operations and limited supporting operations in the physical domains.

2. C&A Roles

a. The DoD Cyber Red Team Accreditation Authority (AA) is the authority to formally approve a DoD Red Team's ability to effectively evaluate a CNDSP or conduct live play on DoD networks. Formal approval is granted via an (Interim) Approval to Operate as described later in this document. USSTRATCOM is the AA for DoD Cyber Red Teams.

b. The DoD Cyber Red Team Certification Authority (CA) manages the process for certifying a DoD Red Team's ability to effectively evaluate a CNDSP. Certification award is in the form of a Certification Award Notice memorandum as discussed later in this document. Director, NSA, is the designated CA and has designated the NSA Cyber Red Team to manage the certification process.

c. The CA uses an evaluation team consisting of at least six members: at least two team members from NSA, and the remaining persons from other accredited DOD Cyber Red Teams. The evaluation team encompasses a subject matter expert from each discipline being evaluated. All evaluation team members must:

(1) Be a current member of an accredited DoD Cyber Red Team. **Note:** A contractor may act as a DoD Cyber Red Team evaluator or consultant and provide technical support and recommendations to the certification and accreditation process, but may not serve in a lead capacity where such participation decides the overall approval or disapproval of a certification.

(2) Meet the minimum grade requirements of E-5 for military and GS-11 for civilians.

(3) Possess an understanding of public law, Federal and DoD policies that apply to DoD Cyber Red Teams, and DoD Cyber Red Team guidance, and possess DoD required certifications.

(4) Have at least 1 year of experience on an accredited DoD Cyber Red Team, knowledge and experience with the DoD Cyber Red Team C&A evaluation methodology and its related processes, and past participation in at least one C&A evaluation as an observing member.

(5) Have a clearance equal to or greater than any information they may come in contact with. At a minimum, members must have a final SECRET clearance.

(6) Be independent of and lack a vested interest in the team being evaluated.

ENCLOSURE B

PHASE I – REGISTRATION

1. Registration

a. This phase consists of three activities: C&A Application Submission, C&A Application Review, and C&A Application Acceptance.

b. The applicant submits application documents to the CA. Upon review, the CA makes the determination to either proceed with the C&A process or continue to work with the applicant to ensure all documentation is in order.

c. The CA establishes an evaluation team consisting of members from accredited DoD Cyber Red Teams. The CA, as the team lead, forwards the applicant's documentation to the evaluation team for review.

2. CA and C&A Evaluation Team Preparation

a. The C&A evaluation team's primary activities during Phase I include identifying information of the assigned mission, key supporting organizations, facilities, team personnel, and contact information, and determining the goals and objectives for the evaluation.

b. During Phase I, the CA shall:

(1) Be the central point of coordination for the evaluation process.

(2) Be the recipient of the applicant's application package.

(3) Collect, guide, and store all metrics, documentation, and audits.

(4) Conduct a review of the required application package.

(5) Notify the applicant and schedule the on-site evaluation.

(6) Coordinate request for evaluation team members and designate a team lead for all certification evaluations. When the NSA Cyber Red Team is due for an evaluation, two team leads are selected from experienced members of accredited DoD Cyber Red Teams not associated with NSA.

(7) Determine the course of action if the preliminary evaluation indicates that the applicant has not met minimum requirements for a C&A evaluation.

c. The C&A evaluation team lead shall:

(1) Provide the C&A evaluation team members with documents and information to review.

(2) Coordinate with the applicant point of contact (POC) to provide any additional information.

(3) Notify C&A evaluation team members of the proposed on-site evaluation schedule. **Note:** An on-site evaluation is conducted at all Cyber Red Team sites. For example, if Service X is requesting that multiple Cyber Red Teams be evaluated at the same time, the evaluation team must go to all locations where the Cyber Red Teams reside.

(4) Develop an evaluation timeline and plan for Phase II activities.

(5) Complete administrative preparations for the Phase II activities.

3. Application Submission. The applicant initiates the C&A evaluation process through formal submission of the application consisting of a Commanding Officer-endorsed letter of request (minimum O-5 or civilian equivalent), self-assessment results, completed application checklist, and all documentation supporting the Evaluator Scoring Metrics (ESM). Documents, templates, and checklists are available on the DoD Cyber Red Team Secure Internet Protocol Router Network (SIPRNET) Web site. Contact the NSA Client Advocate for USCYBERCOM (IE112) at 410-854-5100 for web address.

4. Application Package Review and Acceptance

a. The CA reviews the application to determine if the applicant has met at least the minimum requirements for evaluation. The CA provides a recommendation of acceptance to the C&A evaluation team lead with all accompanying documentation.

b. After the applicant's documentation is accepted, the C&A process proceeds to Phase II, Verification, and the on-site evaluation.

5. Nonconcurrence. Phase I completion may be delayed if the CA or evaluation team identifies potential issues with the applicant's documentation that may negatively impact the applicant's ability to be certified. In this case the CA continues to work with the applicant until all application or documentation issues are resolved.

6. End of Phase I Action Items. Application approval by the CA is a prerequisite for scheduling an on-site evaluation of the applicant.

ENCLOSURE C

PHASE II - VERIFICATION

1. Verification

a. Phase II proceeds following the CA's acceptance of the application. During this phase the C&A evaluation team proceeds to the applicant's site(s) to conduct personnel interviews, site tours, data collection and analyses, observations, and reviews needed to evaluate the applicant as a DoD Cyber Red Team.

b. During Phase II the C&A evaluation team uses performance metrics from the ESM to assess operational effectiveness of the applicant as a DoD Cyber Red Team. The ESM focuses on administration, operations planning and reporting, training, processes and procedures, operations support, and tools. The NSA Cyber Red Team, in coordination with USSTRATCOM and other certified DoD Cyber Red Teams, may adjust the ESM as necessitated by changes in technologies; laws; and tactics, techniques, and procedures. The most current ESM is available on the DoD Cyber Red Team SIPRNET Web site. Contact the NSA Client Advocate for USCYBERCOM (IE112) at 410-854-5100 for a Web site address.

c. Specific C&A evaluation team activities during phase II include:

(1) Provide in-brief to the applicant and staff prior to commencing the evaluation. In-brief shall describe the C&A process and all objectives associated with the evaluation.

(2) Identify, obtain, review, and analyze additional applicant information and documentation as needed.

(3) Utilize the ESM to conduct interviews of key personnel.

(4) Complete the ESM in sufficient detail for preparation of deficiency or certification report. At a minimum, the evaluator must complete scores prior to departing the applicant's site. ESM scores are uploaded to the DoD Cyber Red Team SIPRNET Web site within 7 calendar days after the evaluation is completed.

(5) Provide out-brief containing all findings and recommendations to the applicant and staff.

2. Preevaluation Planning. Planning activities are coordinated by the C&A evaluation team lead and/or an individual designated by the C&A evaluation team lead. The planning activities include the following:

a. Determine the initial scope of the evaluation based upon identified or imposed constraints or limitations specific to the applicant.

b. Develop interview questions based on the applicant's documentation. Questions should supplement the ESM.

c. Provide site location and security clearance requirements to evaluation team members.

3. On-site Evaluation

a. The on-site evaluation determines how the applicant's procedures, processes, and operational activities are conducted within DoD Cyber Red Team C&A requirements.

b. The on-site evaluation process consists of the following actions:

(1) The C&A evaluation team lead provides an in-brief of the C&A process to the applicant's Commanding Officer or designated representative and staff. This briefing includes introduction of the C&A evaluation team to the applicant and other staff.

(2) Interview and discussions conducted with selected technical and support staff.

(3) Completion of the ESM.

(4) Site tours (optional).

(5) At the conclusion of the evaluation, the team lead provides an out-brief to the Commanding Officer or designated representative and staff with the results of the evaluation.

4. Interview Process

a. The applicant provides a finalized on-site interview schedule prior to the arrival of the evaluation team.

b. A nominal list of key on-site personnel is provided for interviews that highlight the following areas: Administration, Operations Planning and Reporting, Operations Support, and Tools. It is incumbent upon the applicant

POC to coordinate the matching of interviews to personnel with responsibilities covered in the ESM. The following personnel should be considered:

(1) Division/Organization Chief

(2) Division/Organization Deputy Chief

(3) Functional Managers

(4) Junior and Senior Operators

(5) Supervisors

(6) Training Personnel

(7) Software Developers

(8) Mission Planning Personnel

(9) Mission Network Specialists

c. Demonstrations. C&A evaluation team members observe demonstrations of critical applicant information systems, assets, tools, and/or key processes and procedures (e.g., tactics, techniques, and procedures) performed by qualified/certified applicant personnel.

5. Evaluation Scoring. The evaluation team scores the applicant's administration, operations and reporting, operations support, and tools in accordance with the ESM. The ESM is a metrics-based document, managed by the NSA and updated in coordination with USSTRATCOM and all accredited DoD Cyber Red Teams, that establishes the minimum standards to operate as a DoD Cyber Red Team on DoD information systems/networks. The scoring methodology is broken down by priority, reflecting the metrics importance, with Priority I being the highest and Priority IV the lowest. Minimum percentages are as follows:

a. Priority I Metric

(1) 100% = Pass

(2) 99% or lower = Fail

b. Priority II Metric

(1) 90% or greater = Pass

(2) 75%-89% = Marginal

(3) 74% or lower = Fail

c. Priority III Metric

(1) 75% or greater = Pass

(2) 50%-74% = Marginal

(3) 49% or lower = Fail

d. Priority IV Metric. Not Graded. Priority IV metrics are "pilot" metrics. For example, if there is a new metric that NSA or USSTRATCOM would like to use to evaluate a DoD Cyber Red Team, they may start it as a Priority IV until it is refined enough to "make it count."

6. Certification Requirements

a. In order to pass certification and be accredited, each applicant must achieve a passing score in all Priority I–III metrics.

b. The CA uses evaluation scores and recommendation from the C&A evaluation team to make a certification determination during Phase III, Validation.

c. Recertifications are conducted on a 3-year cycle, based on the last date of accreditation.

d. An Interim Authority to Operate (IATO) may be granted by the AA for an assessment that receives a marginal score in any area without failures. An IATO must not exceed 180 days. Extensions may be granted by the AA on a case-by-case basis.

(1) Corrective actions that cannot be implemented by the applicant while the C&A evaluation team is on-site must be identified, justified, and provided to the CA in a Plan of Action and Milestones (POA&M), that the CA accepts, within 30-days of the evaluation. The POA&M is endorsed by the first O-6 in the chain of command. **Note**: Conflicts between the CA and applicant are resolved by the AA.

(2) The CA schedules a follow-on evaluation within 120-days of the IATO notification date. The follow-on evaluation assesses the resolution actions implemented by the applicant.

(3) The AA grants accreditation upon successful completion of the follow-on evaluation, as recommended by the CA.

7. DoD Cyber Red Team ESM

a. For each of the applicant's services (i.e., Administration, Operations, Support, and Tool functions), a series of attributes and metrics have been designed to determine the applicant's performance in each of these areas. The current ESM can be found on the DoD Cyber Red Team SIPRNET Web site.

b. The ESM is used by the C&A evaluation team to validate the ability of the applicant to meet the requirements for DoD Cyber Red Team services.

c. Each evaluator scores individual ESMs. If the evaluation team members are unable to reach a consensus on a final score for each metric, the team lead mediates the discrepancy with final authority over the metric score.

8. Pre-Brief to Technical Staff. Prior to the formal out-brief, there is a pre-brief to the applicant POC and key technical personnel. This is the same brief planned for the Commanding Officer.

9. Out-Brief. The C&A evaluation team presents a formal out-brief to senior management and other key staff members. The out-brief is presented in one of two formats, as selected by the applicant's senior management: a) A formal out-brief that is recordable and attributable; or b) An informal out-brief that is not recordable and not attributable. The reason for the formal versus informal out-brief is to stimulate frank discussion on DoD Cyber Red Team findings, as selected by senior management.

(INTENTIONALLY BLANK)

ENCLOSURE D

PHASE III – VALIDATION

1. Validation

a. Phase III is predicated on the certification of the applicant by the CA.

b. The C&A evaluation team prepares Certification and Deficiency Reports for the CA. The CA reviews the reports and makes a certification determination.

c. The CA forwards the reports with a recommendation to the AA. Validation culminates with accreditation by the AA provided to the applicant.

2. Deficiency and Certification Reports. The C&A evaluation reporting process includes a Deficiency Report and a Certification Report.

a. The Team Lead sends the reports to the CA no later than 14 calendar days after return from the evaluated site.

b. The C&A evaluation team lead forwards the final version of the Discrepancy and Certification Reports and recommendation to the CA, who reviews and packages the material for routing to the AA.

c. The Deficiency Report contains identified deficiencies, recommended corrections, timeline for making corrections, and requirements for attaining certification (i.e., when a Priority I metric is failed).

d. The Certification Report contains:

(1) An Executive Summary.

(2) Brief description of the C&A process.

(3) Applicant's ability to provide DoD Cyber Red Team services to its subscribers.

(4) Applicant's critical mission, operations and support, and infrastructure to include identification and justification for those not assessed.

(5) Summary of applicant's services, processes, and security measures assessed.

(6) ESM scores.

(7) Accreditation recommendation.

3. Certification Award Notice and Accreditation Recommendation

a. After the on-site evaluation is complete and the Certification and Deficiency Reports have been submitted to the CA, the CA uses the reports to draft a certification award notice. A copy of the reports and the award notice is sent to the applicant. Certification award notices include a listing of DoD Cyber Red Team services certified by the CA.

b. The reports, the certification award notice, and a letter recommending accreditation of the applicant must be submitted by the CA to the AA no later than 30 days after receipt of the reports from the evaluation team.

4. Accreditation Award. Once the applicant has been recommended for accreditation, the AA reviews the recommendation to ensure the applicant has met all the conditions for accreditation. An Authorization to Operate may be granted for a period of 3 years from the date of certification. The accreditation memorandum is provided to the applicant with copies provided to NSA and the United States Cyber Command. Only the DoD Cyber Red Team identified in the accreditation memorandum is authorized to evaluate a CNDSP or conduct live play on a DoD network (i.e., accreditation of a single Navy Cyber Red Team does not authorize all Navy Cyber Red Teams to evaluate a CNDSP or conduct live play on DoD networks).

ENCLOSURE E

PHASE IV - POST ACCREDITATION

1. Post Accreditation

a. The Post Accreditation Phase includes activities by the accredited DoD Cyber Red Team to maintain C&A status, monitor changes to the DoD Cyber Red Team mission, and prepare and apply for recertification.

b. Periodic self-assessments, not less than annually, shall be conducted during this phase. Recertification and reaccreditation are required at a minimum of every 3 years; when there is a significant change to the DoD Cyber Red Team's operations (see paragraph 3 of this enclosure), policies and procedures, and/or performance levels; or when directed by the AA.

2. Periodic Recertification

a. All accredited DoD Cyber Red Teams must be recertified/reaccredited within 3 years of the accreditation date. To prevent a lapse in C&A, the DoD Cyber Red Team, CA, and AA follow the timeline described below.

(1) Eight months prior to the accreditation expiration date, the CA notifies the DoD Cyber Red Team by official message of the upcoming evaluation.

(2) Six months prior to the accreditation expiration date, the DoD Cyber Red Team is required to submit its application via the registration process.

(3) Four months prior to the accreditation expiration date, the C&A evaluation team performs an on-site pre-evaluation, which determines if the applicant is ready for the formal evaluation.

b. Accreditation extensions must be requested by the DoD Cyber Red Team's Commanding Officer, in writing, to the CA at least 6 months prior to the current accreditation expiration date. The CA evaluates the request and makes an extension recommendation to the AA within 30 calendar days.

3. Recertification. Recertification of accredited DoD Cyber Red Teams is conducted when:

a. The DoD Cyber Red Team’s due date for certification is 4 months out.

b. The DoD Cyber Red Team has acquired new tool suites. The CA determines if a recertification is required and/or if an on-site visit is required.

c. The DoD Cyber Red Team has a requirement to provide a new service that was not previously certified (e.g., wireless assessment).

d. The DoD Cyber Red Team has had a significant turnover of personnel (e.g., 50 percent of the personnel have less than 1 year on the team), or the Commanding Officer has decertified a sufficient number of personnel previously certified to perform critical tasks.

4. Revocation of C&A

a. Accredited DoD Cyber Red Teams that fail to apply for reaccreditation or fail to maintain certification as a result of deficiencies found during a recertification are subject to revocation of their accreditation.

b. Failure to respond to general conditions and agreements of C&A shall be viewed as a basis for revocation of accreditation. The AA, in coordination with the CA and the DoD CIO, makes this decision.

c. DoD Cyber Red Teams that fail to successfully maintain C&A are not authorized to conduct DoD Cyber Red Team operations on any DoD-owned information system/network.

ENCLOSURE F

REFERENCES

a. DoDI 8530.2, 9 March 2001, "Support to Computer Network Defense"

b. Committee on National Security Systems Instruction (CNSSI) No. 4009, 26 April 2010, "National Information Assurance (IA) Glossary"

c. CJCS Execute Order to Incorporate Realistic Cyberspace Conditions into Major DoD Exercises, 11 February 2011

d. CJCSI 6510.01, series, "Information Assurance (IA) and Support to Computer Network Defense (CND)"

e. CJCSM 6510.01, series, "Cyber Incident Handling Program"

f. DoDD O-8530.01, 8 January 2001, "Computer Network Defense (CND)"

g. DoD O-8530.01-M, 17 December 2003, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation (C&A) Program"

h. DoD 8570.01-M (Chg 2), 20 April 2010, "Information Assurance Workforce Improvement Program"

i. DoD 5205.02-M, 3 November 2008, "DoD Operations Security Program Manual"

j. DoDI 8560.01, 9 October 2007, "Communication Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing"

k. "Evaluator Scoring Metrics," V4, 29 December 2011

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

AA	Accreditation Authority
C&A	Certification and Accreditation
CA	Certification Authority
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNDSP	Computer Network Defense Service Provider
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
ESM	Evaluator Scoring Metrics
IATO	Interim Authority To Operate
NSA	National Security Agency
POA&M	Plan of Action and Milestones
POC	Point of Contact

PART II – DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purpose of this instruction only.

Accreditation. Formal declaration by the Accrediting Authority that the Computer Network Defense Service (CNDS) Provider operates at a level meeting or exceeding CNDS certification standards and is approved to provide CNDS in accordance with DODI 8530.2 (reference a).

Certification. An evaluation of the technical and nontechnical services of a Computer Network Defense Service (CNDS) Provider completed in support of the CNDS accreditation process. The evaluation determines the extent a CNDS Provider performs specified CNDS criteria.

Information Assurance (IA). See CNSSI No. 4009 (reference b).

Red Team. See CNSSI No. 4009 (reference b).