DoD Instruction 8585.01

DoD Cyber Red Teams

Originating Component:	Office of the DoD Chief Information Officer
Effective:	January 11, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	John B. Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive 5144.02, this issuance:

- Establishes the DoD Cyber Assessment Program pursuant to:
  - Section 1502 of Title 6, United States Code (U.S.C.).
  - Section 2224 of Title 10, U.S.C.
  - Chapter 35 of Title 44, U.S.C.
- Establishes policy and assigns responsibilities for the DoD Cyber Assessment Program requirements and supporting sub-programs for all DoD Components involved in the development, acquisition, and sustainment of DoD digital infrastructure, systems, and system components under their awareness throughout the system's lifecycle. The policy and procedures:
  - Provide governance for the DoD Cyber Red Team (DCRT) community, mission prioritization, deconfliction, and reporting of findings.
  - Define scope and authorities of DCRTs and assign processes for validating the skills and qualifications of those teams.
  - Assign responsibilities for risk evaluation associated with conducting DCRT assessments and the risks and results associated with the teams that conduct them.
- May affect the policy and responsibilities in Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6510.05 and Manual 6510.03 and supersedes any conflicting guidance in those documents.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the CJCS and the Joint Staff, the Combatant Commands (CCMDs), the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components".

b. The operations and activities of DCRTs that are certified by the National Security Agency (NSA) and accredited by the United States Cyber Command (USCYBERCOM) to conduct cyber operations across the Department of Defense information networks (DoDINs) in support of and as authorized by:

(1) The appropriate DoD Component;

(2) DoDIN area of operations (DAO) commanders;

(3) DAO directors; or

(4) Component authorizing officials (AOs) assigned in accordance with DoDI 8510.01 for the relevant cyber terrain.

1.2. POLICY.

a. DoD cyber assessment teams (DCATs) conduct cyber cooperative, adversarial assessments within specialized settings to determine cyber risk to the DoD when conducting operations in a contested and congested cyberspace.

(1) DCATs are a cyber-focused group of personnel (military, civilian, or contractor) organized and authorized to support a variety of roles germane to the cyber posture of the DoDIN. DCATs may execute operations in support of training, assessments, test, inspections, and other cyber risk determinations.

(2) DCAT operations are subject to authorization by Component-designated AOs to access networks and systems for specific events.

b. DCRTs are a specialized type of DCAT. DCRTs will follow the guidance in this issuance, DoD Instruction (DoDI) 8500.01, DoDI 8530.01, DoDI 8531.01, and DoD Manual 8530.01 to:

(1) Address the governance, prioritization, operations, deconfliction, and reporting of DCRT activities.

(2) Address gaps in existing guidance as identified in the:

(a) DoD Inspector General 2020-067 Audit Report 2020-067.

(b) Report to Congress on the Joint Assessment of DCRT Capabilities, Capacity, Demand, and Requirements in Response to Section 1660 of the National Defense Authorization Act for Fiscal Year 2020.

c. DoD Components that sponsor one or more DCRT will identify a single official responsible for implementing this issuance. Coordination of their DCRT(s) will be conducted as described in USCYBERCOM Standing Ground Rules (SGR) and Section 3 of this issuance.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (CIO).

In addition to the responsibilities in Paragraph 2.11, the DoD CIO, through the Chief Information Security Officer:

a. Develops and publishes revised guidance to update DoD policies, as required, in coordination with the:

(1) Commander, USCYBERCOM (CDRUSCYBERCOM).

(2) Director, NSA/Chief, Central Security Service (DIRNSA/CHCSS).

(3) CJCS.

(4) Stakeholders from OSD and DoD Components.

b. Establishes, manages, and aggregates DoD Components' reporting of DCRT capacity, capabilities, activities, and unmet DCRT requests to:

(1) Inform program budget activities.

(2) Analyze and present DoD Component DCRT capacity, capabilities, activities, and unmet DCRT requests at the USCYBERCOM DCRT annual conference, in coordination with and support from the:

(a) CJCS.

(b) Principal Cyber Advisor (PCA).

(c) Director, Operational Test and Evaluation (DOT&E).

(d) Organizations responsible for the certification and accreditation (C&A) of the DCRTs.

c. Develops a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the Cyber Workforce Management Board (CWMB) in accordance with DoDD 8140.01 in coordination with the:

(1) PCA.

(2) Under Secretary of Defense for Personnel and Readiness (USD(P&R)).

(3) DOT&E.

(4) Organizations responsible for the C&A of the DCRTs

d. Establishes a process to prioritize DCRT support requests in coordination with the DOT&E and DoD Component heads.

e. Approves annual DCRT conference agenda.

f. Develops policies to ensure DCRTs adhere to C&A standards to achieve and maintain an authority to operate (ATO) across DoDIN boundaries.

(1) Adjudicates C&A decision challenges.

(2) Establishes and provides specific guidance for commercial C-ISP exception to policy to be included within the C&A process.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY.

Under the authority, direction, and control of the DoD CIO, in addition to the responsibilities in Paragraphs 2.11. and 2.12., the Director, Defense Information Systems Agency:

a. Provides access to the DoDIN core enterprise and architecture in support of DCRT activities.

b. Facilitates DCRT activities at the DoDIN nodes.

c. Supports the identification, development, and implementation of mitigations and remediation of DCRT event findings for enhancement of DoDIN cybersecurity posture.

2.3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

In addition to the responsibilities in Paragraph 2.11., the Under Secretary of Defense for Research and Engineering develops, maintains, and publishes DoD technology, program protection, engineering, developmental test and evaluation policies, guidance, and procedures for implementing the DoD Cybersecurity Program in accordance with DoDI 8510.01 and use of DCRT in developmental test and evaluation.

2.4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

In addition to the responsibilities in Paragraph 2.11., the Under Secretary of Defense for Acquisition and Sustainment:

a. Oversees DoD Component acquisition program executive offices and program managers to implement cybersecurity policies and requirements introducing the DCRTs as early as possible in the acquisition of information technology and in an integrated manner across the information technology life cycle.

b. Oversees the Strategic Cybersecurity Program in accordance with Section 2224 of Title 10, U.S.C. for weapons systems and associated critical infrastructure.

2.5. UNDER SECRETARY OF DEFENSE FOR POLICY.

In addition to the responsibilities in Paragraph 2.11., the Under Secretary of Defense for Policy:

a. Through the PCA:

(1) Synchronizes, coordinates, and oversees the implementation of the DoD's Cyber Strategy and other relevant policies and planning documents to achieve DoD cyber missions, goals, and objectives.

(2) Supports the development of a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the CWMB in coordination with the:

(a) DoD CIO.

(b) USD(P&R).

(c) DOT&E

(d) Organizations responsible for the C&A of the DCRTs.

(3) Supports the establishment of a process to report DCRT capacity, capabilities, and activities in coordination with the:

(a) DoD CIO.

(b) CJCS.

(c) DOT&E.

(d) Organizations responsible for the C&A of the DCRTs.

(4) Supports DoD CIO development of policy requiring DCRT adherence to C&A standards to achieve and maintain an ATO across DoDIN boundaries.

(5) Supports the annual DCRT conference.

b. Through the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs:

(1) Coordinates all mission assurance policy to ensure the DoD can execute its core missions, in accordance with DoD Directive 3020.40.

(2) Establishes and leads a comprehensive and integrated risk management governance and oversight steering group.

(3) Ensures a mission assurance approach to develop and execute the DoD's Cyber Strategy.

2.6. USD(P&R).

In addition to the responsibilities in Paragraph 2.11., the USD(P&R), through the Chief Talent Management Officer, develops a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the CWMB in coordination with the following stakeholders:

a. DoD CIO.

b. PCA.

c. Organizations responsible for the C&A of the DCRTs.

d. DOT&E.

2.7. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

In addition to the responsibilities in Paragraph 2.11., the USD(I&S) provides exercise planning, policy, and strategic oversight and support for all DoD intelligence, counterintelligence, law enforcement, and security policy, plans, and programs.

2.8. DIRECTOR, DEFENSE INTELLIGENCE AGENCY.

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in Paragraph 2.11., the Director, Defense Intelligence Agency:

a. Conducts all-source analysis of cyber adversary tactics, techniques, and procedures (TTP), including signals intelligence, to develop threat profiles for relevant cyber threat actors.

b. Coordinates with the Directors of National Intelligence and the DoD Special Access Program Central Office to assure DCRT access to information and capabilities necessary to conduct DoD cyber operations.

c. Coordinates with and disseminates all-source signals intelligence products and reports on adversary cyber capabilities and TTPs to the:

(1) CJCS.

(2) CDRUSCYBERCOM.

(3) DIRNSA/CHCSS.

(4) DOT&E.

(5) Defense Counterintelligence Security Agency.

(6) DCRT Chiefs.

2.9. DIRNSA/CHCSS.

Under the authority, direction, and control of the USD(I&S) and the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the NSA, funded through the Information System Security Program, and in addition to the responsibilities in Paragraphs 2.11. and 2.12., the DIRNSA/CHCSS:

a. In coordination with the DoD CIO and DCRT stakeholders, establishes a formal DCRT certification program, providing financial and personnel resources to evaluate the DCRT ability to emulate cyber adversaries and perform DCRT capabilities with minimal risk while operating across DoDIN boundaries.

b. In coordination with the DCRTs stakeholders, and as the DoD certification authority for DCRTs:

(1) Develops and manages the process for certifying DCRTs in accordance with the DCRT C&A Handbook and the DCRT Certification Evaluator's Scoring Metrics for DCRTs.

(2) Submits accreditation recommendations to CDRUSCYBERCOM.

c. Distributes the standards and safeguards for use throughout the DoD to ensure DCRT activities are conducted safely, securely, and with minimal risk to the DoDIN in accordance with applicable laws, regulations, and policies and in coordination with the DoD Component heads.

d. In coordination with the CDRUSCYBERCOM, serves as the final validation authority, for requests by DoD Component organizations to be certified as a DCRT authorized to conduct cyber operations across DoDIN boundaries.

e. Collaborates with applicable DoD Components on the identification, development, and implementation of mitigations and remediation of cyber assessment findings to enhance DoDIN cybersecurity posture.

f. Establishes a DCRT forum in which intelligence and TTP are shared among the DCRT community.

g. Establishes a biannual DCRT "Red Team Huddle" event to facilitate collaboration, technology exchanges, operator leadership development, and education on C&A standards amongst the DCRT community.

h. Reviews and revises certification standards annually, or as needed, to:

(1) Ensure standards are current.

(2) Address standards to qualify cyber personnel to augment certified DCRTs.

i. Supports the DoD CIO to establish a prioritization process for DCRT support requests.

j. Supports the development of a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the CWMB in coordination with the:

(1) DoD CIO.

(2) USD(P&R).

(3) PCA.

(4) DOT&E.

(5) Organizations responsible for the C&A of the DCRTs.

k. Supports the annual DCRT conference.

2.10. DOT&E.

In addition to the responsibilities in Paragraph 2.11., the DOT&E:

a. Provides oversight for cybersecurity testing of systems in development, acquisition, or sustainment for designated programs and tests, including scheduling, planning, execution, and reporting results of specified acquisition DCRT activities.

b. Arranges DCRT support for cybersecurity assessments supporting CCMDs and Military Services and oversees the planning, execution, and reporting of those events.

c. Provides results of acquisition cyber tests to CDRUSCYBERCOM and key stakeholders for inclusion in DoD analysis and reporting of discovered vulnerabilities of DoD systems and information.

d. Provides exercise assessment findings to CDRUSCYBERCOM and key stakeholders for inclusion in DoD analysis and reporting of the impacts to operational systems and missions.

e. Supports the DoD CIO in establishing a prioritization process for DCRT support requests.

f. In coordination with the CJCS and the Combatant Commanders (CCDRs), ensures that cyber opposing force (OPFOR) activities:

(1) Are consistent with, and integrated into, joint exercise environments.

(2) Portray credible cyber threats and reflect a realistic contested cyberspace domain.

g. Provides technical support to CDRUSCYBERCOM for the implementation of a standardized tool development process to ensure the safety, security, reliability, and efficiency of the tools DCRTs will use on the DoDIN.

h. Supports the annual DCRT conference.

i. Supports the development of a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the CWMB in coordination with the:

(1) DoD CIO.

(2) USD(P&R).

(3) USD(P) PCA.

(4) Organizations responsible for the C&A of the DCRTs.

j. Supports the establishment of a process to report DCRT capacity, capabilities, and activities in coordination with the:

(1) DoD CIO.

(2) CJCS.

(3) DOT&E.

(4) Organizations responsible for the C&A of the DCRTs.

2.11. PRINCIPAL STAFF ASSISTANTS AND DOD COMPONENT HEADS.

The Principal Staff Assistants and DoD Component heads:

a. Approve and nominate Component organizations for DCRT C&A in accordance with DoDI 8530.01. Prioritize DoD Component requests, if required.

b. Ensure all organizations performing assess, aggress, inspect, and test (A2IT) operations, activities, and actions (OAA) adhere to the reporting requirements outlined in the current Joint Forces Headquarters-DoDIN (JFHQ-DoDIN) Operation Order 8600 to:

(1) Provide situational awareness of A2IT OAA.

(2) Deconflict A2IT OAA from real-world adversarial activities.

c. Support DCRT operations and activities by providing access to and across the DoDIN enterprise infrastructure (e.g., gateways and nodes).

d. Validate that DoD Component DCRT and augmentees employed externally to another DoD Component's portion of the DoDIN are explicitly authorized by CDRUSCYBERCOM to conduct those operations in accordance with DCRT policies and regulations.

e. Support the DoD CIO to establish a prioritization process for DCRT support requests.

f. Collaborate on the identification, development, and implementation of mitigations and remediation of DCRT event findings for enhancement of DoDIN cybersecurity posture across the DoD with:

(1) NSA.

(2) Military Departments.

(3) USCYBERCOM.

g. Designate or establish a Component Chief Information Security Officer, who will serve as a headquarters-level single focal point to track and document DCRT findings, mitigations, and remediation for inclusion in DoD analysis and reporting of DCRT discovered vulnerabilities that may impact the confidentiality, availability, and integrity of DoD systems and data. Report these findings, mitigations, and remediations to the:

(1) CDRUSCYBERCOM.

(2) Commander, JFHQ-DoDIN.

(3) DOT&E (as required).

(4) Appropriate CCDRs.

(5) Appropriate DoD Component leadership.

(6) DIRNSA/CHCSS

h. Develop and implement:

(1) Processes for providing reports with DCRT findings and recommendations to all organizations and personnel within the DoD Component responsible for corrective actions.

(2) A risk-based process to assess the impact of DCRT-identified vulnerabilities and prioritize funding for corrective actions for high-risk vulnerabilities.

i. Document and report actions taken to accept, mitigate, or remediate all DCRT-identified vulnerabilities.

j. Submit an annual report to the DoD CIO that contains unmet DCRT requests to inform program budget activities by the annual DCRT conference.

k. Participate in the annual DCRT conference.

l. When conducting DCRT operations, provide situational awareness of DCRT activities through trusted-agents or other means as authorized in writing by the CDRUSCYBERCOM. DoD Components implement policy to ensure:

(1) Assigned trusted agents within each applicable node and subcomponent sign a non-disclosure agreement before receiving DCRT information in accordance with USCYBERCOM SGR.

(2) Direct that supervisors and exercise coordinators are made aware of the overall Trusted Agent requirements, their responsibilities, and points of contact to ensure deconfliction of exercise play from real-world activity in accordance with DoDI 3020.47.

(3) Trusted agents will not reveal, without appropriate authorization, from within the Trusted Agent chain-of-coordination, specific information "entrusted" by a DCRT such as when active operations are beginning or ending, internet protocol addresses, host names, usernames, targets, or TTPs.

m. Ensures Commanders and agency directors responsible for enterprise-level DoDIN access (i.e., Internet Access Point architecture) under the authority, direction, and control of the DoD CIO grant access to DCRTs.

2.12. SECRETARIES OF THE MILITARY DEPARTMENTS, COMMANDANT OF THE UNITED STATES COAST GUARD, AND DIRECTORS OF DEFENSE AGENCIES AND DOD FIELD ACTIVITIES WITH DCRTS.

In addition to the responsibilities in Paragraph 2.11. and through the Chief Information Security Officers established in accordance with Paragraph 2.11.h, the Secretaries of the Military Departments, the Commandant of the United States Coast Guard, and the Directors of Defense Agencies and DoD Field Activities with DCRTs:

a. Prescribe the operational chain of command for DCRTs within their organizations.

b. Ensure CCMDs, Military Services, Defense Agencies, and DoD Field Activities employ DCRT resources consistent with operational priorities.

c. Grow DCRTs capabilities through the development and funding of training, resources, and capabilities to emulate real-world adversarial activities.

d. Maintain a capability to execute DCRT activities for employment in single Service, joint, and national-level exercises, operations, acquisition tests and assessments, and other activities.

e. Resource DCRTs to meet joint training standards and maintain competency in using the tools, techniques, and procedures associated with the responsibilities and legal requirements to perform DCRT operations in accordance with USCYBERCOM SGR.

f. Collaborate on the identification, development, and implementation of mitigations and remediation of DCRT findings to enhance DoDIN cybersecurity posture with:

(1) OSD.

(2) Applicable DoD Components.

(3) USCYBERCOM.

g. Support collaboration efforts to share information between DCRTs, as established by the CDRUSCYBERCOM.

h. Validate DoD Component DCRTs and augmentees employed externally to another DoD Component's portion of the DoDIN are authorized by the CDRUSCYBERCOM to conduct those operations in accordance with DCRT policies and regulations.

i. Collaborate with other DCRTs regarding tools, techniques, and procedures.

j. Ensure DoD Component-initiated DCRT activities are conducted in accordance with USCYBERCOM SGR.

k. Ensure planned DCRT operations are coordinated with the CDRUSCYBERCOM and are in accordance with this issuance. The respective Service cyber component commander will perform this function for training and assessments and a specified acquisition entity will perform this function for acquisition penetration tests.

l. Establish capability development plans for supporting DCRT growth over the near, medium, and long term. These plans:

(1) Address:

(a) The implementation of the tailored recruitment plan for military, civilian, and internship personnel regarding the acquisition and retention of personnel.

(b) The expansion of team capacity.

(c) The development of new capabilities and training infrastructure.

(2) Are synchronized across the DoD to support joint requirements.

m. Ensure DCRTs are trained to conduct cyber activities safely and securely while operating on the DoDIN, and in accordance with DCRT policy and guidance.

n. Incorporate:

(1) Persistent and realistic cyber threats to support training and exercises for continued development and assessment of offensive and defensive cyberspace and DoDIN operations in accordance with CJCS Guide 3500.01.

(2) To the greatest extent possible, DCRT operations and activities into exercises, games, and research conducted through the Joint Military and Service Education Enterprise.

o. Establish internal processes in accordance with DCRT guidance, DoDI 8531.01, and CJCS Manual 6510.01 to share the findings of DCRT assessments with relevant stakeholders, including:

(1) CDRUSCYBERCOM.

(2) Commander, JFHQ-DoDIN.

(3) DOT&E (as required).

(4) CCDRs.

(5) Other applicable DoD Components heads.

(6) Appropriate DoD Component leadership.

p. Provide annual and on demand reporting to the DoD CIO in support of strategic planning for DCRT resourcing requirements. The report will include, but is not limited to, capacity, capabilities, activities, and unmet DCRT requests. The annual report is due by July 10.

q. Establish and fund the means for developing, collecting, cataloging, maintaining, and distributing tools for DCRTs in accordance with CDRUSCYBERCOM guidance.

(1) Ensure DCRTs provide access to the body of evidence for their respective tool kits upon request by USCYBERCOM and DOT&E.

(2) Any DCRT employing tools under the auspices of this issuance must remain compliant with all applicable CDRUSCYBERCOM mandated policies and safeguards.

r. Support the DoD CIO to establish a prioritization process for DCRT support requests.

s. Identify highly sensitive missions and systems protection requirements and coordinate with the CDRUSCYBERCOM to ensure DCRT tool kits are compliant.

t. Participate in the annual DCRT conference.

2.13. CJCS.

In addition to the responsibilities in Paragraph 2.11., the CJCS:

a. In coordination with CCDRs and the DOT&E, ensures cyber OPFOR activities are consistent with, and integrated into, joint exercise environments, portraying credible cyber threats and reflecting a realistic contested cyberspace domain.

b. In coordination with the CDRUSCYBERCOM and DOT&E, implements a standard and joint tool development process that will establish the safety, security, reliability, and efficiency of the tools DCRTs will operate on the DoDIN.

c. Supports the annual DCRT conference.

d. Analyzes DoD Component DCRT capacity, capabilities, activities, and unmet DCRT requests for information to ensure CCMD and Combat Support Agency equities are represented.

2.14. CCDRS.

In addition to the responsibilities in Paragraph 2.11., and through the CJCS, the CCDRs:

a. Maintain awareness of all DCRT activities within their area of responsibility.

b. Review and provide guidance for engagements with DCRTs.

c. Participate in the annual USCYBERCOM conference to review DCRT capacity, capabilities, activities, and unmet DCRT requests.

d. Support a high state of mission readiness in the CCMD using one or more cyber OPFOR in continuous exercises and other training activities as considered appropriate.

e. Ensure DCRT activities align to joint and combined operations.

f. Participate in mission approval boards for DCRT activities conducted in support of operational vulnerability assessments and exercises in their operating area in accordance with USCYBERCOM SGR.

g. Prioritize joint exercises in coordination with the DCRT requirements of the:

(1) CJCS.

(2) DIRNSA/CHCSS.

(3) Secretaries of the Military Departments.

(4) CDRUSCYBERCOM.

(5) DOT&E (as required).

h. Identify cyber OPFOR support for planning and execution of joint exercises through the CJCS Joint Training Information Management System.

2.15. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraphs 2.11. and 2.14., the CDRUSCYBERCOM:

a. Establishes a formal DCRT accreditation program, providing financial and personnel resources needed to support C&A activities, in addition to authorizing DCRTs to emulate cyber adversaries across DoDIN boundaries.

b. Serves as the DoD accreditation authority for DCRTs and manages the accreditation process for authorizing DCRTs to execute cyber operations across DoDIN boundaries.

c. Tracks DCRT activities, and deconflicts as needed, to maintain situational awareness of operations affecting the DoDIN.

d. Provides guidance for DCRT activity reporting.

e. In coordination with the DIRNSA/CHCSS, establishes and implements Joint Training Standards to define minimum operator training standards for DCRTs and better support augmentation between DCRTs.

f. Provides operational guidance to DAO commanders and directors.

g. Supports the DoD CIO to establish a prioritization process for DCRT support requests.

h. In coordination with DoD stakeholders, oversees component reporting of DCRT findings and mitigations.

i. Coordinates with the Commander, JFHQ-DoDIN and the DoD Component heads on a process to identify and track mitigations of cyber assessment findings until resolved.

j. Establishes processes to ensure coordination and sharing of information between DCRTs.

k. Publishes guidance for DoD Components with DCRTs to collect, catalog, maintain, and distribute DCRT tools across the DCRT community.

l. In coordination with the CJCS, the DOT&E and the DoD Component heads who own DCRTs, develops and implements a standardized tool development process for the tools DCRTs use as part of their assessments.

(1) The process will be submitted and overseen by the Information Security Risk Management Committee for Risk Management Framework Enterprise ATO in accordance with DoDI 8510.01. This ensures any CDRUSCYBERCOM-accredited DCRT operating on a DoD network will not require a risk management framework ATO for tool kits employed in pursuit of their assigned mission objectives.

(2) Request access to the DCRT body of evidence for their respective tool kits as necessary.

m. In coordination with the certification authority, develops, manages, and updates the accreditation processes for DCRTs.

n. Supports the development of a tailored recruitment plan for military, civilian, and internship personnel to expand DCRT expertise for approval at the CWMB in coordination with the:

(1) DoD CIO.

(2) USD(P&R).

(3) PCA.

(4) DOT&E.

(5) Organizations responsible for the C&A of the DCRTs.

o. Supports the establishment of a process for reporting DCRT capacity, capabilities, activities, and unmet DCRT requests in coordination with the:

(1) DoD CIO.

(2) PCA.

(3) DOT&E.

(4) CJCS.

p. Coordinates an annual conference that includes key stakeholders to review the annual reporting of capacity, capabilities, activities, and unmet DCRT requests.

q. Requires DCRTs to report significant changes in personnel status to ensure operational capabilities can be met in accordance with CDRUSCYBERCOM ATO.

r. Reviews and revises USCYBERCOM SGR, as necessary.

SECTION 3: PROCEDURES

3.1. OVERVIEW

a. DCRTs are a specialized type of DCAT that perform a vast array of cyber missions for the DoD. DCRT operations are subject to authorization by Component-designated AOs to access enclaves and systems for specific events.

b. A DCRT is a multi-disciplinary group of personnel (military, civilian, or contractor) organized and authorized to:

(1) Emulate a potential adversary's exploitations or attack capabilities against a targeted mission or capability.

(2) Highlight vulnerabilities and demonstrate operational impact for improving joint operations in cyberspace and the cybersecurity posture of the DoDIN.

c. DCRTs are authorized to conduct cyber operations across DoDIN boundaries when performing:

(1) Acquisition Tester (Tester).

(2) Operational Vulnerability Assessor (Assessor).

(3) Cyber OPFOR Aggressor (Aggressor).

d. DCRTs can support operational and developmental tests of networks, systems, or resources for vulnerabilities that internal or external actors may exploit to impact the confidentiality, integrity, and availability of DoD information or systems.

e. DCRT operations involve all data formats including internet protocol and other data formats, as well as specialized technologies and capabilities (e.g., radio frequency, control systems, cross-domain solutions, weapons systems, non-internet protocol data formats, and data links).

3.2. ROLES.

DCRTs must perform these three distinctive roles (unless waived by the DoD CIO) as part of the DoD defensive cyberspace forces.

a. Acquisition Tester (Tester).

(1) DCRTs conduct adversarial cyber tests of or through a system, service, or enclave exploiting identified vulnerabilities and other weaknesses in coordination with an operational test agency or a developmental test organization, or the program management office (PMO).

(2) While engaged, DCRT actions can be conducted openly and in collaboration with the system or mission owners. Threat-based capabilities and rigorous methodologies are used to assess systems under acquisition, enclaves, and networks in an operationally representative threat environment. These create operational effects through the identification and exploitation of vulnerabilities in systems under acquisition testing.

b. Operational Vulnerability Assessor (Assessor).

(1) DCRTs conduct assessments on live operational networks, either in support of mission assessments or specific acquisition testing in support of a test organization or PMO.

(2) DCRTs conducting this role assess the protective posture of operational networks, systems, and cybersecurity service providers as they emulate adversaries. While engaged, only trusted agents are aware of the specific DCRT actions being performed.

c. Cyber OPFOR Aggressor (Aggressor).

(1) DCRTS operate on networks working closely with the exercise control cell and within the exercise's established rules of engagement (ROE) on a tempo geared to the training audience and objectives.

(2) Aggressors serve as the Cyber OPFOR for exercises emulating and, if possible, replicating a specific key cyber threat actor's capability and TTPs. Where necessary, aggressors will impose mission effects to deny, disrupt, or degrade operations as authorized by the exercise control cell. Cyber OPFOR provides feedback on performance to units as necessary to maximize training.

3.3. PLANNING AND SCHEDULING.

a. When DCRT services do not overlap with cyber mission forces (CMF) (e.g., for test and evaluation or other discrete events) clients may schedule directly with the DCRT.

b. When DCRT services may overlap with CMF, DoD clients should enter a request for support with USCYBERCOM in accordance with USCYBERCOM GENADMIN 22-0120 to deconflict DCRT and CMF tasks. JFHQ-DoDIN will be tasked to provide a sourcing solution by the USCYBERCOM Force Management Office.

c. Trusted agents will be employed by DCRTs to assist in higher planning, coordination, or evaluation of DCRT activities.

3.4. REPORTING.

a. DCRTs will adhere to the reporting requirements outlined in Appendix 4 to Annex R to JFHQ-DoDIN Operational Order 8600 to provide situational awareness of A2IT OAA and to deconflict A2IT OAA from real-world and adversarial activities.

b. DCRT assessment findings and mission reports highlight how an adversary could exploit known and unknown systems or network vulnerabilities to deny, degrade, disrupt, or destroy the DoD's warfighting functions. DCRT assessment findings provide critical threat and vulnerability information to commanders, directors, and other key decision makers to create effective mitigation and defense actions and plans.

c. DCRT assessment findings and reports must be submitted in accordance with:

(1) This issuance.

(2) CJCS Manual 6510.01.

(3) USCYBERCOM SGR.

d. DCRT assessment findings must be reported to the DoD Component or requesting organization upon the completion of DCRT activity. The report will provide a detailed description of identified vulnerabilities, exploits, methods, and any mission effects achieved during the assessment.

3.5. ORGANIZATIONS RECEIVING DCRT SERVICES.

Upon completion of the exercise or activity, the DoD Component and applicable trusted agents will:

a. Make and submit all reports based on approved agreements outlined in the mission's ROE and in accordance with USCYBERCOM SGR.

b. Submit all assessment reports to the DoD CIO Chief Information Security Officer and DoD Cyber Security Service Providers to validate findings have been effectively remediated and mitigated.

c. Receive formal feedback from DCRT (e.g., briefing, report) on the security of the intended cyberspace in support of the organization's exercise or network assessment objectives.

d. Create a plan of actions and milestones that includes a risk mitigation plan highlighting how and when the organization will correct the findings of the DCRT.

e. Send a formal DCRT after-action report, to include the plan of actions and milestones, in accordance with the USCYBERCOM SGR and this issuance.

f. Ensure network has been reset for future exercises or network assessments, including destroying technical references created during the DCRT activity that list DCRT internet protocols and signatures and any blocks of DCRT internet protocol addresses.

g. Report that all reset actions have been completed to JFHQ-DoDIN in accordance with USCYBERCOM SGR.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
A2IT	assess, aggress, inspect, and test
AO	authorizing official
ATO	authority to operate
CCDR	Combatant Commander
CCMD	Combatant Command
CDRUSCYBERCOM	Commander, United States Cyber Command
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CMF	cyber mission forces
CWMB	Cyber Workforce Management Board
C&A	certification and accreditation
DAO	DoDIN area of operations
DCAT	DoD cyber assessment team
DCRT	DoD Cyber Red Team
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoDI	DoD instruction
DoDIN	Department of Defense information network
DOT&E	Director, Operational Test and Evaluation
JFHQ-DoDIN	Joint Forces Headquarters-Department of Defense Information Network
NSA	National Security Agency
OAA	operations, activities, and actions
OPFOR	opposing force
PCA	Principal Cyber Advisor
PMO	program management office
ROE	rules of engagement
SGR	standing ground rules
TTP	tactics, techniques, and procedures
U.S.C.	United States Code
USCYBERCOM	United States Cyber Command

ACRONYM	MEANING
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
Acquisition Tester (Tester)	An individual or organization conducting adversarial cyber tests of or through a system, service, or enclave exploiting identified vulnerabilities and other weaknesses in coordination with an operational test agency, developmental test organization, or PMO. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
Cyber OPFOR Aggressor (Aggressor)	An individual or organization operating on networks working closely with the exercise control cell and within the exercise's established ROE on a tempo geared to the training audience and objectives. Aggressors serve as the Cyber OPFOR for exercises emulating and, if possible, replicating a specific key cyber threat actor's capability and TTPs. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
cybersecurity	Defined in Committee on National Security Systems Instruction Number 4009.
DCAT	Cyber assessment teams that execute operations in support of training that include assessments, tests, inspections, and other cyber risk determinations. DCATs conduct cyber assessments in cooperative, adversarial, and specialized settings to determine cyber risk to the DoD when conducting operations in a contested cyber environment. Operations are subject to authorization by Component-designated AOs assigned in accordance with DoDI 8510.01 to access networks and systems for specific events. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
DCRT	Teams certified by the NSA and accredited by the USCYBERCOM to conduct cyber operations across the DoDIN in support of and as authorized by the appropriate DoD Component, DAO commanders, DAO directors, and AOs for the relevant cyber terrain. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
DoDIN	Defined in the DoD Dictionary of Military and Associated Terms.
joint training and certification standards	Defined in the "Joint Training & Certification Standards (JT&CS) for Cyber Red Teams and Units Responsible for the Cyber Defense of Control Systems".
Operational Test and Evaluation	Defined in Section 139 of Title 10, U.S.C.
Operational Vulnerability Assessor (Assessor)	An individual or organization conducting assessments on live operational networks, in support of mission assessments, specific acquisition testing or in support of a test organization or PMO. Those conducting this role assess the protective posture of operational networks, systems, and cybersecurity service providers as they emulate adversaries. This term and its definition are approved for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.
risk tolerance	Defined in Committee on National Security Systems Instruction Number 4009.

REFERENCES

Chairman of the Joint Chiefs of Staff Guide 3500.01, "Chairman's Guidance for Training and Exercise Support to Global Integration," January 31, 2019

Chairman of the Joint Chiefs of Staff Instruction 6510.05, "Department of Defense Cyber Red Teams," May 15, 2018

Chairman of the Joint Chiefs of Staff Manual 6510.01, "Cyber Incident Handling Program," current edition

Chairman of the Joint Chiefs of Staff Manual 6510.03, "Department of Defense Cyber Red Team Certification and Accreditation," February 28, 2013

Committee on National Security Systems Instruction Number 4009, "Committee on National Security Systems (CNSS) Glossary", March 7, 2022

DoD Cyber Strategy, 2018

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Inspector General Audit Report DoDIG-2020-067, March 13, 2020

DoD Instruction 3020.47, "DoD Participation in the National Exercise Program (NEP)," January 29, 2019

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020

DoD Manual 8530.01, "Cybersecurity Activities Support Procedures," May 31, 2023

Joint Forces Headquarters-Department of Defense Information Network Operations Order 8600, Appendix 4 to Annex R, "Red Team Deconfliction," current edition

Joint Training & Certification Standards (JT&CS) for Cyber Red Teams and Units Responsible for the Cyber Defense of Control Systems, current edition[1]

National Security Agency, "DoD Cyber Red Team Certification and Accreditation (C&A) Evaluator's Scoring Metrics," current edition

Principal Cyber Advisor, DoD CIO, and DOT&E Fiscal Year 2020 National Defense Authorization Act Section 1660 Report to Congress, "Report on Joint Assessment of Department of Defense Cyber Red Team Capabilities, Capacity, Demand, and Requirements in Response to Section 1660 of the National Defense Authorization Act for Fiscal Year 2020," December 16, 2020

[1] Available to authorized users at https://intelshare.intelink.sgov.gov/sites/jfhq-dodin/J3/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/jfhq-dodin/J3/OPORD8600/OPORD%208600-22%20FRAGORD%202%20Annex%20R%20Appendix%204%20(Red%20Team%20Deconfliction)_27OCT22%20(CUI).pdf&action=default

United States Code, Title 6, Section 1502

United States Code, Title 10

United States Code, Title 44, Chapter 35

United States Cyber Command, "DoD Cyber Red Team Certification and Accreditation (C&A) Handbook," current edition[2]

United States Cyber Command GENADMIN 22-0120, "Standard Operating Procedures (SOPS) for Request for Support to U.S. Cyber Command," current edition[3]

United States Cyber Command Operational Guidance, "Standing Ground Rules for DoD Cyber Red Team Operations on the DoDIN," current edition[4]

[2] Contact the certification authority.

[3] Available to authorized users at https://intelshare.intelink.sgov.gov/sites/usybercom/RFS_Documents/GENADMIN2022-0120.pdf

[4] Available to authorized users at https://intelshare.intelink.sgov./sites/cybercom/orders/Orders/Forms/Other.aspx