DoW Instruction 3600.03

Test and Evaluation of Cyberspace Effects and Enabling Capabilities

Originating Component:	Office of the Under Secretary of War for Research and Engineering
Effective:	July 15, 2026
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction O-3600.03, "(U) Test and Evaluation of Cyberspace Effects and Enabling Capabilities," January19, 2022
Approved 07/08/2026 by:	Emil Michael, Under Secretary of War for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, this issuance:

- Establishes policy, assigns responsibilities, prescribes procedures, and provides a standardized evaluation framework for test and evaluation (T&E) of cyberspace effects and enabling capabilities (CEEC), including cyber weapons.
- Establishes a three-tiered governance structure for CEEC T&E, including the DoW Component-led DoW CEEC T&E Working Group (WG).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 3
1.1. Applicability. 3
1.2. Policy. 3
SECTION 2: RESPONSIBILITIES 4
2.1. Under Secretary of War for Research and Engineering (USW(R&E)). 4
2.2. Under Secretary of War for Acquisition and Sustainment. 5
2.3. Under Secretary of War for Policy (USW(P)). 5
2.4. Assistant Secretary of War for Cyber Policy. 5
2.5. DOT&E. 5
2.6. DoW Component Heads. 7
2.7. CJCS. 8
2.8. CCDRs. 9
2.9. Commander, USCYBERCOM. 10
SECTION 3: GOVERNANCE STRUCTURE 11
3.1. Structure. 11
a. Tier I. 11
b. Tier II. 11
c. Tier III. 13
3.2. Tiered Organizational Functions. 13
a. Tier I Functions. 13
b. Tier II Functions. 13
c. Tier III Functions. 14
SECTION 4: CEEC T&E FRAMEWORK, SCOPE, AND PROCEDURES 15
4.1. Introduction. 15
a. Purpose. 15
b. CEEC T&E Framework. 15
4.2. CEEC T&E Scope. 16
4.3. Implementation. 17
4.4. Procedures. 18
4.5. CEEC T&E Artifact Repositories. 19
4.6. Exceptions to Policy. 19
APPENDIX 4A: CEEC T&E WAIVER OF SPECIFIC TEST STANDARDS REQUEST TEMPLATE 21
GLOSSARY 22
G.1. Acronyms. 22
G.2. Definitions. 22
REFERENCES 30

TABLE

Table 1. Standardized CEEC T&E Framework 12

FIGURES

Figure 1. Governance Structure for CEEC T&E 11
Figure 2. CEEC T&E Waiver of Specific Test Considerations Request Template 21

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSW, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoW Field Activities, and all other organizational entities within the DoW (referred to collectively in this issuance as the "DoW Components").

b. This issuance does not apply to and does not alter the National Security Agency's authority to test and evaluate cyberspace-based signals intelligence capabilities.

1.2. POLICY.

The DoW providers of CEEC, both acquired and organically developed, will:

a. Implement T&E for CEEC in accordance with DoD Instructions (DoDIs) 5000.89 and 5000.98 and DoD Manuals 5000.96 and 5000.99. CEEC T&E includes:

(1) Developmental test and evaluation (DT&E) (e.g., DT&E performed by the system developer, contractor, or government);

(2) Operational test and evaluation (OT&E); or

(3) Integrated testing.

b. Implement the standardized CEEC T&E framework using DoW Component best practices modified to the operational environment and supported mission in advance of operational employment.

c. Provide Combatant Commanders (CCDR), or their designee, with a consistent measurable degree of confidence that the evaluated CEEC performs as designed and will provide the CCDR or their designee with the required mission capabilities in the operational environment.

d. Employ standardized CEEC T&E frameworks updated and managed by the DoW CEEC T&E WG to enable T&E result acceptance by all DoW Components.

e. Scope and schedule CEEC evaluations appropriately to meet capability delivery timelines, operational needs and required performance, and resource constraints.

f. Classify CEEC in accordance with DoDI O-3600.02, the United States Cyber Command (USCYBERCOM) Consolidated Security Classification Guide 5210.01, or the DoW Component's governing security classification guide.

g. Mark and handle CEEC reports containing controlled unclassified information using appropriate category markings in accordance with DoDI 5200.48.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF WAR FOR RESEARCH AND ENGINEERING (USW(R&E)).

The USW(R&E):

a. Establishes and maintains DT&E policies and ensures the DoW Components maintain appropriate test facilities, test ranges, tools, and related modeling and simulation capabilities, in support of CEEC.

b. Serves as the lead for the development of modifications to this issuance, in conjunction with the Director of Operational Test and Evaluation (DOT&E) and in accordance with DoDI 5025.01.

c. In conjunction with the DOT&E, the USW(R&E):

(1) Leads the development of, and co-approves, the DoW CEEC T&E WG Charter pursuant to Paragraph 3.2.b.

(2) Reviews and updates the DoW CEEC T&E WG Charter at least every 2 years and as necessary.

(3) Appoints the Chair for the DoW CEEC T&E WG every 2 years from among nominated candidates and in coordination with the Commander, USCYBERCOM.

(4) Co-sponsors any sub-WGs (if established) of the DoW CEEC T&E WG and participates as an advisor.

(5) Reviews the annual summary reports consolidated by the DoW CEEC T&E WG to monitor DoW-wide CEEC T&E standardization compliance and to identify process and resource shortfalls.

(6) Coordinates with the DoW Components that are developing or sponsoring CEEC for the DoW Component to designate:

(a) A DoW CEEC T&E WG representative from the respective DoW Component.

(b) An authoritative, single point of contact for the respective DoW Component's CEEC T&E policies, procedures, evaluations, and evaluation results.

d. Reviews and comments on each DoW Component's CEEC implementation procedures and processes for their compliance with this issuance.

e. Approves the DT&E plan in the T&E master plan (TEMP) in accordance with DoDD 5137.02 for every Acquisition Category 1D program associated with CEEC.

f. Advises the milestone decision authority on the DT&E plan in the TEMP, test strategy, or other overarching program test planning documents for Acquisition Category 1B or 1C programs associated with CEEC listed on the T&E Oversight List for DT&E (available at https://www.dote.osd.mil/Oversight/).

g. Ensures adequate T&E infrastructure is available to accomplish CEEC T&E processes in a timely and comprehensive manner.

2.2. UNDER SECRETARY OF WAR FOR ACQUISITION AND SUSTAINMENT.

The Under Secretary of War for Acquisition and Sustainment:

a. Ensures acquisition policies reference CEEC T&E policies where applicable.

b. Designates a representative to serve on the DoW CEEC T&E WG.

2.3. UNDER SECRETARY OF WAR FOR POLICY (USW(P)).

The USW(P) reviews and comments on the annual summary report consolidated by the DoW CEEC T&E WG.

2.4. ASSISTANT SECRETARY OF WAR FOR CYBER POLICY.

Under the authority, direction, and control of the USW(P), the Assistant Secretary of War for Cyber Policy, in their role as the Principal Cyber Advisor as designated in the March 20, 2024, Deputy Secretary of Defense Memorandum:

a. Acts as the Principal Cyber Advisor to the Secretary of War on military cyber forces and activities.

b. Develops, coordinates, assesses, and oversees the implementation of DoW cyberspace policy and strategy which guides DoW efforts in CEEC in accordance with the March 20, 2024, Deputy Secretary of Defense Memorandum.

c. Represents the USW(P) in the DoW CEEC T&E WG and provides feedback on the annual summary report consolidated by the WG on behalf of the Office of the USW(P).

2.5. DOT&E.

The DOT&E:

a. Provides the Secretary of War, Congress, and operational acceptance authorities with assessments of the effectiveness, suitability, survivability, and other attributes of CEEC on the T&E Oversight List for OT&E across the full spectrum of military operations pursuant to Sections 139 and 4171 of Title 10, United States Code, and DoDD 5141.02.

b. Advocates to ensure the availability of DoW test facilities and test ranges to support CEEC OT&E and independently advises the Secretary of War and the USW(R&E) on CEEC OT&E capability deficiencies identified as:

(1) OT&E limitations or

(2) Realistic full spectrum T&E limitations.

c. For CEEC programs under DOT&E oversight, approves TEMPs and operational test plans and assesses the adequacy of OT&E performed by:

(1) The Military Services.

(2) Operational test agencies.

(3) Any other DoW entity performing OT&E.

d. Establishes, integrates, and advocates for adequacy of realistic full spectrum guidelines and best practices as needed to enable end-to-end mission relevant evaluations.

e. In conjunction with the USW(R&E), the DOT&E:

(1) Assists the development of, and co-approves, the DoW CEEC T&E WG Charter pursuant to Paragraph 3.2.b.

(2) Reviews and assists in updating the DoW CEEC T&E WG Charter at least every 2 years and as necessary.

(3) Advises on the selection of the Chair for the DoW CEEC T&E WG every 2 years from among nominated candidates and in coordination with the Commander, USCYBERCOM.

(4) Co-sponsors any sub-WGs of the DoW CEEC T&E WG (if established) and participates as an advisor.

(5) Reviews annual summary reports aggregated by the DoW CEEC T&E WG to monitor the overall DoW-wide CEEC T&E standardization compliance and identify process and resource shortfalls.

(6) Coordinates with the DoW Components developing or sponsoring CEEC for the DoW Component to designate:

(a) A DoW CEEC T&E WG representative from the respective DoW Component.

(b) An authoritative, single point of contact for the respective DoW Component's CEEC T&E policies, procedures, evaluations, and evaluation results.

f. Reviews and comments on each DoW Component's CEEC implementation procedures and processes for their compliance with this issuance.

2.6. DOW COMPONENT HEADS.

In accordance with the DoW Component's implementation guidance and procedures, the DoW Component heads designate the organization to serve as the DoW Component CEEC lead (e.g., the Service Cyber Component) with the authority and responsibility to:

a. Ensure programs, projects, and activities developing, acquiring, or sponsoring CEEC, plan, budget, and provide all necessary resources for the T&E activities required by this issuance.

b. Provide oversight of CEEC development and T&E efforts within their respective DoW Component.

c. Develop, update, and maintain DoW Component implementation guidance and procedures to designate roles and responsibilities, and establish T&E procedures for CEEC in accordance with this issuance, the DoD Test and Evaluation Enterprise Guidebook, and the DoD CEEC T&E Standards Guidebook.

d. Designate representatives from the DoW Component T&E organizations to the DoW CEEC T&E WG to advise on T&E matters related to CEEC.

e. Nominate individuals to serve as the DoW CEEC T&E WG Chair every 2 years and provide nominee names and endorsements to the USW(R&E) and DOT&E for review and selection.

f. Monitor compliance with, and modifications to, the DoD CEEC T&E Standards Guidebook.

g. Participate in the CEEC Community of Practice (CoP) and direct CEEC developers, testers, operators, and evaluators to leverage the CoP to capture best practices for T&E. Encourage proposals for modifications to the CEEC T&E framework, standards descriptions, metrics, methodologies, applicability, and exclusions to the DoW CEEC T&E WG.

h. Submit and manage CEEC T&E waiver requests to, and in coordination with, the appropriate CCDR in accordance with Paragraph 2.8. of this issuance. Adjustments to the T&E framework in Table 1 may be made based on:

(1) The acquisition pathway.

(2) Available resources.

(3) The size, risk, and complexity of the CEEC under development.

(4) The area of cyberspace (high side, blue space, red space, or gray space) where the mission is employed or observed.

i. Ensure T&E organizations conduct CEEC T&E, document the results, and retain all CEEC T&E artifacts. Handle any personally identifiable information and controlled unclassified

information contained in CEEC test artifacts and repository records in accordance with Section 552(a) of Title 5, United States Code, also known and referred to in this issuance as "the Privacy Act of 1974," DoDI 5400.11, and DoDI 5200.48.

j. Leverage the National Cyber Range Complex provided by the Test Resource Management Center whenever reasonable. The National Cyber Range Complex offers multiple U.S. locations at no cost, providing a closed, tailorable, and reusable environment for CEEC T&E activities. These ranges address infrastructure needs, support operational mission tempo, and ensure consistency in testing processes across DoW Components.

k. Ensure Tier III teams, described in Paragraphs 3.1.c. and 3.2.c. of this issuance, coordinate DT&E and OT&E when integrated testing is not feasible to facilitate synergy of test resources and sharing of data and results.

l. Document and report T&E results for all approved, currently operational, and future CEEC. Deliver artifacts to the repository maintained by the requiring CCDR or Commander, USCYBERCOM. DoW Component implementation guidance must describe anticipated CCDR repository requirements.

m. Test and evaluate risks in the CEEC development environment against known cyber threats, including:

(1) Developer processes, tools, and test environments (e.g., coding, testing, identity and access management, and supply chain risk management).

(2) Secure capabilities (e.g., software patching, encryption, and configuration control).

n. Incorporate CEEC into DoW Component, joint, or combined experiments and exercises to enhance operational readiness and interoperability. Incorporating CEEC must be done in consultation with the exercise owner and informed by a risk assessment of safety and potential impacts to exercise objectives. The exercise owner decides whether to accept or reject the incorporation based on the results of the consultation and risk assessment.

o. Prepare and submit annual summary reports to the DoW CEEC T&E WG to inform the USW(R&E) and the DOT&E of compliance with this issuance.

2.7. CJCS.

In addition to the responsibilities in Paragraph 2.6., the CJCS:

a. Coordinates CCDR submissions for the CEEC annual report.

b. Participates in the DoW CEEC T&E WG.

2.8. CCDRS.

In addition to the responsibilities in Paragraph 2.6., the CCDRs:

a. Employ CEEC either under Commander, USCYBERCOM authorities or under the CCDR's authorities.

b. Approve CEEC T&E modifications to meet operational mission tempo and the CCDR's intent.

c. For CEEC employment under the CCDR's authorities, may waive one or more, but not all, specific CEEC T&E considerations due to emergency situations.

d. For waivers of one or more, but not all, specific CEEC T&E considerations for CEEC employment under Commander, USCYBERCOM authorities, submit a waiver request to the Commander, USCYBERCOM. Figure 2 in Appendix 4A provides the Commander, USCYBERCOM waiver template.

e. For CCDR CEEC capabilities, plan for and support operational employment by:

(1) Supporting OT&E by providing access to operationally realistic environments, threats, and personnel within their area of responsibility.

(2) Developing concepts of operations and tactics, techniques, and procedures, and integrating validated capabilities into operational and contingency plans upon successful completion of T&E.

f. Establish a repository, and associated metadata requirements, to provide storage of all T&E documents, test artifacts, and waivers for approved, existing operational, and future CCDR unique CEEC. Facilitate cybersecurity enforcement and information technology management of the CCDR repository and its cybersecurity service provider.

g. Review CEEC T&E results from their subordinate headquarters and all assigned and attached forces used to prepare capabilities for use in military operations.

h. Incorporate CEEC into DoW Component, Joint, or combined experiments and exercises, to the maximum extent possible.

i. Coordinate with DoW Component heads to determine T&E results of CEEC intended for employment using the CCDR's authorities or infrastructure and CEEC acceptance into existing and future cyber warfighting platforms for operational employment.

j. Coordinate with DoW Component CEEC evaluators to conduct combat assessment in accordance with CJCS Instruction 3162.02.

k. Submit DoW CEEC T&E WG annual report inputs to the DoW CEEC T&E WG of CEEC employed under a waiver as described in Paragraphs 2.8.c. and 2.8.d.

l. Coordinate with other CCDRs as appropriate for CEEC T&E implicating another CCDR's area of responsibility.

2.9. COMMANDER, USCYBERCOM.

In addition to the responsibilities in Paragraphs 2.6. and 2.8., the Commander, USCYBERCOM:

a. Coordinates with the CCDRs and DoW Component heads to facilitate and participate in CEEC T&E activities.

b. Enables standardization of CEEC T&E across the DoW by:

(1) Leading the development and maintenance of all critical operational issues to resolve through the standardized CEEC T&E framework.

(2) Providing the CEEC T&E CoP with the current concepts of operation, operational mode summaries, and mission profiles required to determine the DT&E criteria (e.g., critical technical parameters and key performance parameters) associated with CEEC specific critical operational issues.

(3) Providing technical leadership in developing the best practices for observing, measuring, and evaluating CEEC T&E criteria.

(4) Integrating DoW Component CEEC development and T&E elements into USCYBERCOM's Joint Development Environment, as appropriate.

c. Provides endorsements to the USW(R&E) and the DOT&E for review and selection of the DoW CEEC T&E WG Chair every 2 years.

d. Approves or denies all CCDR requests for waivers for CEEC T&E.

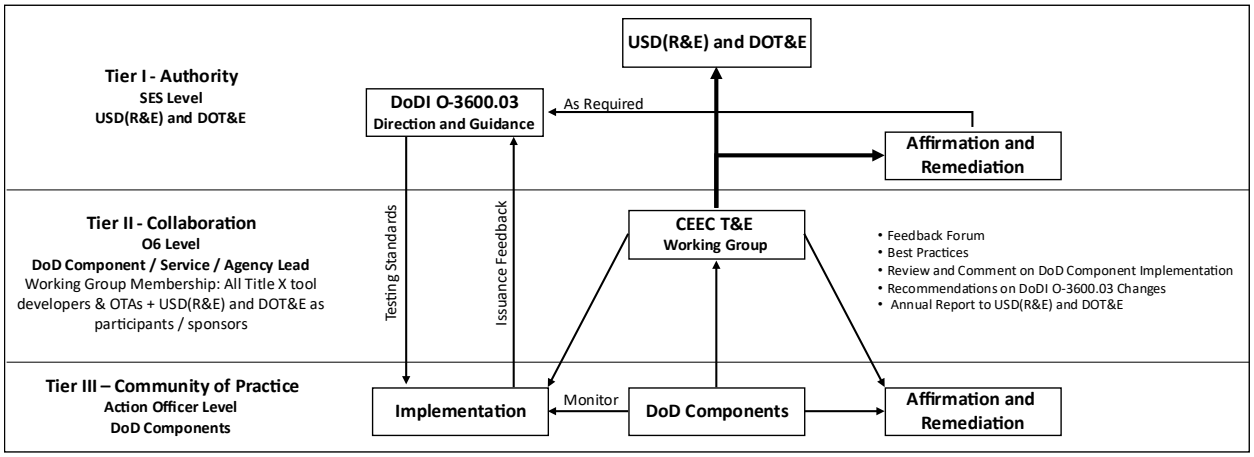
e. Develops and publishes a process for CCDRs to obtain a CEEC T&E waiver due to emergency situations or operational constraints.

SECTION 3: GOVERNANCE STRUCTURE

3.1. STRUCTURE.

Figure 1 depicts the governance structure for CEEC T&E. It consists of three levels of related activities.

Figure 1. Governance Structure for CEEC T&E



a. Tier I.

Tier I is responsible for:

(1) Overseeing the implementation of the procedures and governance in this issuance (e.g., the DoW CEEC T&E WG Charter, publication of the DoD CEEC T&E Standards Guidebook) across the DoW, in accordance with Paragraphs 2.1. and 2.5.

(2) Providing the DoW Components guidance; monitoring the execution of the guidance; and, when required, making appropriate adjustments to the guidance.

b. Tier II.

Tier II is the DoW CEEC T&E WG and is responsible for:

(1) Keeping pace with the dynamic nature of cyberspace operations while continuing to achieve the policies stated in Paragraph 1.2.

(2) Coordinating and organizing the CoP and its associated sub-WGs.

(3) Responding to Tier I inquiries of the CoP.

(4) Establishing, maintaining, updating, and recommending to Tier I the descriptions, T&E standards, metrics, methodologies, applicability, and exclusions for each test consideration specified in Table 1, representing the standardized CEEC T&E framework, for publication in the DoD CEEC T&E Standards Guidebook.

(5) Facilitating and monitoring DoW Component Tier III implementation activities, in accordance with Paragraph 2.6.

(6) Developing, maintaining, and updating the DoW CEEC "Critical Information and Indicators List" and an operations security plan in accordance with DoDD 5205.02E and DoD Manual 5205.02.

Table 1. Standardized CEEC T&E Framework

Test Consideration	Typically applies to this category of CEEC:			Potentially Observable Location:			
	Attack Capability	Platform	Access or Enabling Capability	High Side	Blue Space	Gray Space	Red Space
Attribution	X	X	X		X	X	X
Availability	X	X	X	X	X	X	X
Combat Assessment						X	X
Battle Damage Assessment	X						X
Collateral Damage Assessment	X		X		X	X	X
Munitions Effectiveness Assessment	X	X	X	X	X	X	X
Command and Control	X	X	X	X	X	X	X
Compatibility and Interoperability	X	X	X	X	X	X	X
Configuration Management	X	X	X	X	X	X	X
Co-optability	X	X	X		X	X	X
Cybersecurity	X	X	X	X	X	X	X
Detectability	X		X			X	X
Maintainability	X	X	X	X	X	X	X
Mission Environment	X	X	X	X	X	X	X
Misuse	X	X	X	X	X	X	X
Mobility	X	X	X		X	X	X
Performance	X	X	X	X	X	X	X
Reliability	X	X	X	X	X	X	X
Safety	X	X	X	X	X	X	X
Security	X	X	X	X	X	X	X
Supportability	X	X	X	X	X	X	X
Susceptibility	X	X	X		X	X	X
Sustainability	X	X	X	X	X	X	X
Training	X	X	X	X	X	X	X
Usability	X	X	X	X	X	X	X
Vulnerability (Excludes Cybersecurity)	X	X	X	X	X	X	X

c. Tier III.

Tier III is the CoP and is responsible for:

(1) Implementing the DoW Component published procedures, applying the CoP standards during CEEC T&E implementation, and monitoring the results.

(2) Affirming the CEEC T&E procedures and standards or providing recommendations for remediation or improvement to their Tier II organization and representative.

3.2. TIERED ORGANIZATIONAL FUNCTIONS.

a. Tier I Functions.

Tier I will:

(1) Develop and maintain this issuance, including the authority to modify this issuance in accordance with DoDI 5025.01.

(2) Charter the DoW CEEC T&E WG and be active members and advisors, to include resolving disputes.

(3) Provide advocacy for CEEC T&E adequacy and resourcing (e.g., funding, infrastructure, manpower, tools, and training), ensuring that all advocated capabilities are based on adversary threats validated by the Defense Intelligence Enterprise.

(4) Approve and publish the DoD CEEC T&E Standards Guidebook.

b. Tier II Functions.

Under the leadership of the appointed Chair, the DoW CEEC T&E WG will:

(1) Facilitate WG activities in support of this issuance.

(2) Establish the CEEC T&E CoP and manage access to the CEEC T&E CoP website. The CEEC T&E CoP website:

(a) Is accessible to authorized individuals by coordinating with Tier II.

(b) Contains the DoD CEEC T&E Standards Guidebook.

(c) Enables collaboration across the working-level practitioners and action officers regarding CEEC T&E activities.

(d) Enables documenting and providing best practices, lessons learned, and sharing other resources for CEEC T&E planning, execution, evaluation, and analysis.

(e) Provides the template and data requirements for the CEEC T&E annual summary reports to Tier III.

(3) Develop and submit to Tier I recommended revisions to the current DoD CEEC T&E Standards Guidebook as a companion to this issuance. The guidebook provides specific and current descriptions, T&E standards, metrics, methodologies, applicability, and exclusions, for evaluation and characterization of each test consideration specified in Table 1, representing the standardized CEEC T&E framework.

(4) Establish and direct sub-WGs composed of DoW Component CEEC technical subject matter experts from the CoP, as required.

(5) Deliver annual reports to the Tier I summarizing inputs from Tier III regarding:

(a) Applicability of the standardized CEEC T&E framework.

(b) CEEC T&E impacts on fielding activities.

(c) Identified CEEC T&E gaps (e.g., resources, infrastructure).

(d) Recommendations to address gaps and improve CEEC T&E processes.

(e) Descriptions and timelines of CEEC employed under a CCDR waiver used as explained in Paragraph 2.8.b. or Paragraph 2.8.c.

(f) Proposed changes to this issuance.

(6) Review proposed changes to this issuance and make recommendations to Tier I on their disposition.

(7) Review DoW Component CEEC T&E products to ensure consistent implementation of the CEEC T&E framework across the DoW.

(8) Provide basic guidelines to, and resolve disputes or issues raised by Tier III and sub-WGs or committees related to CEEC T&E. If not resolved, escalate to Tier I for resolution.

c. Tier III Functions.

The CEEC T&E CoP will:

(1) Conduct CEEC T&E, document, and report CEEC T&E results and deliver artifacts to the appropriate CCDR's repository.

(2) Submit input to the Tier II organization and representative for the annual report.

(3) Participate in sub-WGs when requested by Tier II.

SECTION 4: CEEC T&E FRAMEWORK, SCOPE, AND PROCEDURES

4.1. INTRODUCTION.

a. Purpose.

The purpose of the standardized CEEC T&E framework is to provide CCDRs with the critical information necessary to employ any DoW Component's CEEC with operational confidence. DoW Components enable this confidence through:

(1) Collaborative test planning, execution, and data collection to support independent developmental and operational evaluations.

(2) Employing a joint body of practice, evidence, transparency, and consistency throughout CEEC T&E planning, execution, and reporting.

(3) Linking the standardized CEEC T&E framework and T&E results to functional requirements and operational employment decision criteria. This linkage fosters collaboration between DoW Components and increases the likelihood of CEEC acceptance into existing or future cyber warfighting platforms for operational employment.

(4) Promoting inter-Component collaboration to enhance CEEC T&E standardization and:

(a) Facilitate CEEC operational employment through efficient T&E processes.

(b) Enable a standardized T&E approach to inform risk to and support cyberspace operations.

(5) Supporting CCDR development of concepts of operations and tactics, techniques, and procedures for CEEC operational employment by providing CCDRs with timely and comprehensive results from all relevant T&E activities, to include developmental, operational, and integrated T&E.

b. CEEC T&E Framework.

Table 1 provides the standardized CEEC T&E framework. The DoD CEEC T&E Standards Guidebook provides test consideration descriptions, standards, metrics, methodologies, applicability, and exclusions. To build confidence that a CEEC is operationally effective, suitable, and ready for employment, the T&E process will evaluate the system against the CEEC T&E Considerations identified in Table 1. Applying this framework provides:

(1) A common understanding of test criteria, planning, processes, and results among DoW Components, test organizations, and operators as documented in the DoW CEEC T&E WG CoP website.

(2) Common approaches and methodologies for CEEC T&E, as documented in the DoD CEEC T&E Standards Guidebook, and higher confidence in results.

4.2. CEEC T&E SCOPE

a. Plan and conduct DT&E and OT&E for all applicable test considerations in Table 1. CEEC includes:

(1) Cyberspace attack platforms (e.g., Joint Common Access Platform and other delivery platforms) capabilities, in accordance with Joint Publication 3-12, exercised to support the full spectrum of cyberspace operations to:

(a) Create noticeable (either immediately or latent) denial effects (i.e., degradation, disruption, and destruction) in cyberspace or

(b) Enable manipulation which leads to denial effects in the physical domain.

(2) Cyberspace exploitation capabilities, including electromagnetic spectrum-enabled, space-enabled, artificial intelligence-enabled, or machine learning-enabled capabilities.

b. CEEC applies to and may encompass more than:

(1) Software, firmware, and hardware directly used to conduct cyberspace effects operations.

(2) Platforms developed or apportioned for cyberspace effects and monitoring cyberspace attack activities, in accordance with Chapter 19 of Title 10, United States Code.

(3) All intermediate enabling capabilities which are part of the end-to-end mission (e.g., cyberspace exploitation capabilities, electromagnetic spectrum-enabled access capabilities).

(4) Any compiled or scripted code employing decision logic to cause an attack effect. This includes artificial intelligence and machine learning-enabled logic.

c. CEEC excludes:

(1) Unmodified, publicly available software, firmware, and hardware.

(2) Tactics, techniques, and procedures that may involve the use of CEEC, a target's native functionality, inherent capabilities, or installed utilities.

(3) Other items approved by the Tier I governance authorities and awaiting inclusion in this issuance.

4.3. IMPLEMENTATION.

a. In accordance with Paragraph 2.6., DoW Component CEEC leads will apply respective DoW Component DT&E and OT&E implementation guidance, procedures, and processes to measure and evaluate the test data under relevant CEEC test considerations listed in Table 1:

(1) As part of T&E activities conducted during the experimental research, development, equipping, and fielding process for CEEC.

(2) Before operational fielding or employment of CEEC.

b. This issuance does not invalidate existing operational and approved CEEC, nor prior testing and employment approval decisions. The DoW Component CEEC lead will assess all new developments and new fielding or employment approvals of those capabilities in accordance with this issuance.

c. The DoW Component CEEC lead provides the standing guidance regarding retest requirements driven by CEEC modifications (e.g., modification of CEEC, modification of non-CEEC into CEEC, and use of externally sourced capabilities, either beyond their original scope or beyond evidence of their testing).

(1) CEEC developers and testers must provide appropriate awareness to the DoW Component CEEC lead regarding CEEC updates, modifications, or other changes (e.g., target environment changes).

(2) CEEC developers and testers should:

(a) Review changes to CEEC since the last test conducted.

(b) Verify risks associated with the planned modification, to include its development environment, implications for mission risk, and continued mission priority, to develop a recommendation for whether to retest. Provide all recommendations for retest of a CEEC, communicated in terms of mission risk, to the designated DoW Component CEEC lead for review and approval.

(3) The DoW Component CEEC lead provides the standing guidance regarding retest requirements driven by CEEC modifications (e.g., modification of CEEC, modification of non-CEEC into CEEC, and use of externally sourced capabilities, either beyond their original scope or beyond evidence of their testing). Guidance should address implications for:

(a) Development, security, and operations.

(b) Continuous implementation and delivery.

d. CEEC evaluators must be able to conduct an independent evaluation of the CEEC and:

(1) Determine whether the CEEC meets its technical requirements and objectives as established in CEEC documentation.

(2) Document under what operational and environmental conditions the CEEC would fail to meet mission requirements.

(3) Conduct continuous evaluation of employed capabilities using operationally derived data.

4.4. PROCEDURES.

DoW Component CEEC leads and subordinate test organizations will, for each CEEC capability:

a. Conduct a formal hazards and safety risk assessment prior to finalizing the T&E plan. This assessment will identify potential interactions with critical infrastructure and high-consequence systems (including, but not limited to, nuclear weapon systems, nuclear command and control systems, and associated power systems) and will be used to establish strict test boundaries, constraints, and risk-based exclusions.

b. Review the standardized CEEC T&E framework for potential applicability and modification.

(1) Modify, as required, the standardized CEEC T&E framework (see Table 1) during CEEC T&E activities based on:

(a) The type of CEEC (platform, access, or capability).

(b) Specific operational requirements.

(c) Planned end-to-end mission thread.

(d) Operational urgency.

(e) Hazards and safety risk assessment results.

(2) Approve the modified CEEC T&E framework for a given capability and associated end-to-end mission thread before proceeding to testing. Decisions on test consideration applicability will inform recommendations to the DoW CEEC T&E WG regarding future addition or removal of test considerations.

c. Create and maintain documentation annotating the rationale for the modified CEEC T&E framework.

(1) This documentation must annotate the applicable test consideration. Provide a detailed rationale for any test consideration determined not to be applicable.

(2) During testing, the testers will make every reasonable effort to adequately address test considerations pertinent to the system(s) under test.

(3) The testers will identify and explain test constraints and limitations in the TEMP or equivalent documents, test plans, or reports with an emphasis on explaining any test consideration deemed applicable but not adequately tested.

d. Support independent reviews of CEEC T&E adequacy, sufficiency, and commonality to appropriately move toward joint cyberspace operations. DoW Components must:

(1) Make test artifacts and documentation generated by CEEC T&E activities available to the DoW CEEC T&E WG.

(2) Retain and store such material in the appropriate repository or repositories.

e. When practical, perform integrated testing in applying the standardized CEEC T&E framework as described in the DoD CEEC T&E Standards Guidebook.

f. Ensure DoW Component processes evolve, as needed, to comply with and enable the joint cyber warfighting architecture and subsequent offensive cyber operations architecture. Once the architecture is operational, DoW Components must submit the tested and evaluated CEEC, and their associated test artifacts, into the system.

4.5. CEEC T&E ARTIFACT REPOSITORIES.

Repositories for CEEC T&E data will be available for:

a. External review, upon request to authorized individuals.

b. Use by other testers.

c. Other purposes (e.g., cyber training), as needed.

d. Artifacts and repositories that include information about individuals or other sensitive information will be marked and handled in accordance with the requirements of the Privacy Act of 1974, DoDIs 5400.11, and 5200.48.

4.6. EXCEPTIONS TO POLICY.

Only the CCDR has the authority to waive CEEC T&E before fielding or employment under their authorities, in accordance with Paragraph 2.8.

a. DoW Component CEEC leads submit waivers for CEEC T&E in accordance with Paragraph 2.8.

b. Waivers will not serve as a mechanism to bypass application of the standardized CEEC T&E framework or assessing test considerations.

c. The Commander, USCYBERCOM will grant or deny all requests for any waivers received from other CCDRs.

d. DoW Component CEEC leads will complete and document the T&E for any applicable test consideration bypassed via a specific CCDR waiver. In addition, the lead will oversee the DoW Component processes to capture, analyze, and summarize results, lessons learned, and unintended consequences of waivers. These summaries will be included in the annual report submitted to:

(1) The CEEC T&E WG Chair, in accordance with Paragraphs 2.6.o. and 3.2.b.(5).

(2) Any associated stakeholders.

APPENDIX 4A: CEEC T&E WAIVER OF SPECIFIC TEST STANDARDS REQUEST TEMPLATE

Figure 2. CEEC T&E Waiver of Specific Test Considerations Request Template

[OFFICE LETTERHEAD]

MEMORANDUM FOR <ORGANIZATION REQUESTING WAIVER>

SUBJECT: Cyberspace Effects and Enabling Capabilities Test and Evaluation Considerations Waiver Request for <capability name> in Support of <Operation/Cyber Team> Missions

REFERENCES:
(a) <Insert reference>

1. <Provide a summary of the operational urgency and supporting technical justification for waiving test and evaluation (T&E) of the [capability name, version]>

2. <Capability Description/Overview>: <capability name> is a <capability type> which <capability description>.

3. <Provide a discussion supporting assessment of the operational risk of fielding the capability without T&E.>

4. <The requesting Combatant Commander requests a length of time for the waiver, which can be unlimited. The Commander, United States Cyber Command will adjudicate the amount of time granted along with the overarching request as defined by policy.>

5. <Provide a discussion on any previous testing conducted of the capability or assessment information of prior capability version. If applicable, provide a summary of capability developer testing conducted.>

6. <CCMD legal review, assessment, and applicability of signatory's authority to sign this waiver>

7. <Primary point of contact for listed capabilities>

<Signature block of the Combatant Commander> <or>
<Signature block of Designee>

cc:
Under Secretary of War for Research and Engineering
Director of Operational Test and Evaluation

<Note: Incorporate appropriate classification markings when developing the waiver request in accordance with applicable classification guide.>

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CCDR	Combatant Commander
CEEC	cyberspace effects and enabling capabilities
CJCS	Chairman of the Joint Chiefs of Staff
CoP	community of practice
DoW	Department of War
DoDD	DoD directive
DoDI	DoD instruction
DOT&E	Director of Operational Test and Evaluation
DT&E	developmental test and evaluation
OSW	Office of the Secretary of War
OT&E	operational test and evaluation
T&E	test and evaluation
TEMP	test and evaluation master plan
USCYBERCOM	United States Cyber Command
USW(R&E)	Under Secretary of War for Research and Engineering
USW(P)	Under Secretary of War for Policy
WG	working group

G.2. DEFINITIONS.

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

TERM	DEFINITION
access	The tools and techniques for gaining sufficient exposure to, connectivity to, or entry into a device, system, network, or person to further operations.
Acquisition Category 1D, 1B, or 1C	Defined in the Warfighting Acquisition University Glossary.

TERM	DEFINITION
artifact	Documentation, data, and evidence generated or utilized during the T&E process to support decision-making and compliance. These include test plans, results, technical reports, risk assessments, and other materials that demonstrate system performance, effectiveness, suitability, survivability, and adherence to requirements. Artifacts are integral to documentation for developmental, operational, and integrated testing activities.
attribution	The potential to identify the source, purpose, and originator of a capability or action concretely, or through plausible inference inherent in a capability and the data generated by the capability.
availability	Defined in the Warfighting Acquisition University Glossary.
battle damage assessment	Defined in the DoD Dictionary of Military and Associated Terms.
blue space	Denotes areas in cyberspace protected by: a. The United States and its mission partners. b. Other areas the DoW may be ordered to protect.
cyberspace capability	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
CEEC	Cyberspace capabilities developed for use under Title 10, United States Code, authorities, which include standalone cyberspace attack and cyberspace exploitation capabilities. These capabilities encompass electromagnetic spectrum-enabled, space-enabled, artificial intelligence-enabled, and machine learning-enabled functionalities designed to support the full spectrum of cyberspace operations. CEEC are employed to create noticeable (either immediate or latent) denial effects (e.g., degradation, disruption, and destruction) in cyberspace or to generate effects in cyberspace that contribute to outcomes in other domains. Cyberspace exploitation capabilities under CEEC are designed to conduct intelligence activities, maneuver, information collection, and other preparatory actions that enable Combatant Commanders to deliver future cyberspace effects. Activities conducted under non-Title 10, United States Code, authorities, including those governed by Title 50, United States Code, are excluded from this definition unless explicitly authorized and aligned with Title 10, United States Code, operational frameworks.
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.
collateral damage assessment	The evaluation and estimation of the potential unintended harm or disruption a capability might cause to non-targeted systems, individuals, or organizations, essentially assessing the "spillover" effects of an operation beyond the intended target, often including civilian infrastructure or data not directly related to the attack objective.
combat assessment	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
command and control	Defined in the DoD Dictionary of Military and Associated Terms.
compatibility	Defined in the Warfighting Acquisition University Glossary.
configuration management	Defined in the Warfighting Acquisition University Glossary.
cybersecurity	Defined in the Warfighting Acquisition University Glossary.
cyberspace attack	Defined in the DoD Dictionary of Military and Associated Terms.
cyberspace exploitation	Defined in the DoD Dictionary of Military and Associated Terms.
detectability	The ability to discover, notice, or otherwise identify a capability.
developer	An individual who designs, creates, tests, and maintains CEEC or systems to meet operational requirements.
electromagnetic spectrum	A maneuver space consisting of all frequencies of electromagnetic radiation (oscillating electric and magnetic fields characterized by frequency and wavelength). The electromagnetic spectrum often organizes using frequency bands, based on certain physical characteristics. The electromagnetic spectrum includes radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays.

TERM	DEFINITION
end-to-end mission relevant evaluation	A comprehensive assessment conducted across the entire CEEC lifecycle from initial development through operational deployment, to ensure its effectiveness, suitability, survivability, and alignment with mission requirements. These evaluations encompass all critical, technical and operational parameters, including developmental and operational testing, integration into mission threads, and performance in realistic operational environments. The goal is to provide decision-makers with actionable insights into the capability's readiness and impact on achieving mission objectives while identifying and mitigating risks associated with its deployment.
evaluator	A designated individual or team responsible for assessing the performance, technical requirements, operational effectiveness, suitability, or survivability of systems or capabilities. This role supports developmental, operational, or integrated tests by planning, executing, and reporting on evaluations, applying established evaluation frameworks to ensure compliance with DoW policies, requirements, and standards. This role also supports CEEC post-employment evaluations. Evaluators provide objective analysis and issue final ratings to inform acquisition decisions and operational readiness.
gray space	All cyberspace not meeting the description of either “high-side,” “blue space,” or “red space.”
high side	Protected enclave in blue cyberspace, typically separated from the Internet by an air gap or controlled interface such as a Cross-Domain Solution.
integrated testing	Defined in DoDI 5000.89.
interoperability	Defined in DoDI 8330.01.

TERM	DEFINITION
Joint Development Environment	USCYBERCOM collaborative, secure, and integrated network used to design, develop, test, and refine CEEC. It facilitates coordination across military services, agencies, and partners, leveraging shared resources, tools, and expertise to ensure interoperability, scalability, and alignment with operational requirements and strategic objectives.
maintain	The ongoing process of preserving, updating, and ensuring the accuracy, relevance, and effectiveness of existing policy, procedures, and guidance. This includes continuous monitoring, periodic reviews, and necessary modifications to align with evolving policies, standards, and operational requirements, without necessarily making substantial revisions.
maintainability	Defined in the Warfighting Acquisition University Glossary.
mission environment	The set of conditions that a system must experience to complete its mission, to include the relevant threat. It can refer to the physical environment, such as a building, or the general mood of an organization. It can also refer to the ambient conditions a system will experience during its life cycle, such as thermal, electromagnetic, electrostatic, or radiation effects.
misuse	The wrong or improper use of something.
munitions effectiveness assessment	Defined in the DoD Dictionary of Military and Associated Terms.
mobility	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
operational acceptance authorities	Responsible for approving the transition of systems, capabilities, or technologies from development to operational use. These authorities ensure that systems meet established operational requirements, readiness criteria, and mission needs through rigorous evaluation, testing, and validation processes. They oversee the final decision-making for operational fielding, ensuring compliance with DoW policies, standards, and strategic objectives.
operational mission tempo	The pace, intensity, and frequency of military operations conducted by units to achieve mission objectives. It encompasses offensive, defensive, and stability support activities, balancing current operational demands with readiness for future contingencies.
operational test agency	Defined in the Warfighting Acquisition University Glossary.
operations security plan	Defined in DoD Manual 5205.02.
operator	Defined in the Warfighting Acquisition University Glossary.
performance	Defined in the Warfighting Acquisition University Glossary.
platform	Combinations of hardware, firmware, and software from which cyberspace attack activities are planned, executed, monitored, assessed, and reported.
red space	Refers to those portions of cyberspace owned or controlled by an adversary or an enemy.
reliability	Defined in the Warfighting Acquisition University Glossary.
safety	Defined in the Warfighting Acquisition University Glossary.
security	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
Service Cyber Component	The organizational entity within a Military Service that operates under the authority of Commander, USCYBERCOM responsible for planning, executing, and supporting cyberspace operations, including defensive, offensive, and operational preparation of the environment, to ensure mission assurance and enhance the Department of Defense information network security.
standardize	To bring into conformity with a standard especially to assure consistency and regularity.
standards	Defined in the Warfighting Acquisition University Glossary.
standardization	Defined in DoD Manual 4120.24.
supportability	Defined in the Warfighting Acquisition University Glossary.
sustainability	Defined in the Warfighting Acquisition University Glossary.
tester	Defined in the Warfighting Acquisition University Glossary.
training	Defined in the Warfighting Acquisition University Glossary.
update	Actively making significant changes to existing content by incorporating new information, addressing emerging issues, or reflecting changes in policies, procedures, and guidance.
usability	The degree to which something is able or fit to be used.
vulnerability	Defined in the Warfighting Acquisition University Glossary.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3162.02, "Methodology for Combat Assessment," current edition

Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Assistant Secretary of Defense for Cyber Policy," March 20, 2024

DoD Cyberspace Effects and Enabling Capabilities Test and Evaluation Standards Guidebook, August 1, 2024[1]

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5141.02, "Director of Operational Test and Evaluation (DOT&E)," February 2, 2009

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Instruction O-3600.02, "Information Operation (IO) Security Classification Guidance," November 28, 2005

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020

DoD Instruction 5000.98, "Operational Test and Evaluation and Live Fire Test and Evaluation," December 9, 2024

DoD Instruction 5025.01, "DoW Issuances Program," January 20, 2026

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems," September 27, 2022

DoD Manual 4120.24, "Defense Standardization Program (DSP) Procedures," September 24, 2014, as amended

DoD Manual 5000.96, "Operational and Live Fire Test and Evaluation of Software," December 9, 2024

DoD Manual 5000.99, "Realistic Full Spectrum Survivability and Lethality Testing," December 9, 2024

DoD Manual 5205.02, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008, as amended

DoD Test and Evaluation Enterprise Guidebook, August 19, 2022[2]

Joint Publication 3-12, "Joint Cyberspace Operations," December 19, 2022

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

[1] Available on the CEEC T&E WG CoP hosted at https://www.trmc.osd.mil/

[2] Available at https://www.dote.osd.mil/Portals/97/pub/policies/2022/TE%20Enterprise%20Guidebook%208.02.pdf?ver=_oHESMId4chfhi-sTtSqLw%3d%3d

United States Code, Title 5

United States Code, Title 10

United States Code, Title 50

United States Cyber Command Guide 5210.01, "Consolidated Security Classification Guide," November 27, 2024[3]

Warfighting Acquisition University Glossary, "Glossary of Defense Acquisition Acronyms and Terms", current edition[3]

[4] Available at https://www.waru.edu/glossary