DoD Manual 5000.99

Realistic Full Spectrum Survivability and Lethality Testing

Originating Component:	Office of the Director of Operational Test and Evaluation
Effective:	December 9, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Director of Operational Test and Evaluation Memorandum, "Cyber Economic Vulnerability Assessments (CEVA)," January 21, 2015 Director of Operational Test and Evaluation Memorandum, "Operational Test and Evaluation (OT&E) of Electromagnetic Environmental Effects (E3) and Spectrum Management", October 25, 1999 Director of Operational Test and Evaluation Memorandum, "Enterprise Cloud Adoption – Operational Test Considerations," October 1, 2018 Director of Operational Test and Evaluation Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," April 3, 2018
Approved by:	Douglas C. Schmidt, Director of Operational Test and Evaluation

Purpose: In accordance with the authority in DoD Directive (DoDD) 5141.02 and the policy in DoD Instruction (DoDI) 5000.98, this issuance implements policy, assigns responsibilities, and provides procedures for realistic full spectrum survivability and full spectrum lethality testing of DoD systems and services (referred to in this issuance as "DoD systems") acquired via the Defense Acquisition System or via other non-standard acquisition systems.

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. The OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of 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. DoD systems acquired via the Defense Acquisition System, pursuing any adaptive acquisition framework pathway in accordance with DoDD 5000.01 and DoDI 5000.02.

c. DoD systems under special access controls in accordance with DoDD 5205.07.

d. Non-standard acquisition systems (e.g., missile defense system).

1.2. POLICY.

a. In accordance with DoDI 5000.98, the DoD will plan, fund, execute, and report on realistic testing required to evaluate full spectrum survivability and full spectrum lethality, as applicable, of DoD systems in contested, congested, and constrained operational environments using live kinetic and non-kinetic threats and targets.

b. Realistic full spectrum survivability and full spectrum lethality testing includes the evaluation of full spectrum survivability and lethality effects on operational effectiveness, including, but not limited to, communications, firepower, and mobility, suitability, and collateral damage, as applicable.

c. Realistic full spectrum survivability and lethality planning, execution, analysis, and reporting will use the latest Intelligence Community knowledge and will be conducted against operationally representative and relevant kinetic and non-kinetic threats and targets, as applicable, within the program's expected life cycle. Examples include:

(1) Kinetic.

(2) Cyber.

(3) Electromagnetic spectrum (EMS) including directed energy weapons and doctrinally appropriate force structures to evaluate congested and constrained environments.

(4) Chemical, biological, radiological, and nuclear (CBRN).

(5) Other operationally relevant kinetic and non-kinetic threats and targets including, but not limited to, artificial intelligence (AI)-based threats and data storage targets.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR OF OPERATIONAL TEST AND EVALUATION (DOT&E).

Pursuant to Sections 139, 4171, 4172, and 4231 of Title 10, United States Code; Section 223 of Public Law 117-81; and DoDI 5000.98, the DOT&E reviews and approves exceptions and procedural deviations from this issuance for acquisition programs on the Test and Evaluation (T&E) Oversight List for operational test and evaluation (OT&E) and live fire test and evaluation (LFT&E).

2.2. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)).

The USD(R&E) assesses the adequacy and approves developmental test and evaluation (DT&E) strategies documented in the Test and Evaluation Master Plan (TEMP), T&E strategy, or equivalent document, referred to in this issuance as "TEMP/T&E strategy," for acquisition category ID programs under T&E oversight for DT&E. For all other acquisition programs under DT&E oversight, the USD(R&E) advises the milestone decision authority by conducting an independent analysis of test data, reports, modeling and simulation (M&S) results, and the adequacy of the DT&E plan in the TEMP/T&E strategy.

2.3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)).

The USD(A&S):

a. Enforces this issuance for DoD systems for which the USD(A&S) is the milestone decision authority.

b. Establishes processes that mitigate and remedy vulnerabilities discovered in operationally fielded DoD systems subject to this issuance.

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

The USD(I&S) oversees intelligence support to the acquisition life cycle and advises the DOT&E concerning intelligence supportability requirements that affect OT&E and LFT&E.

2.5. DOD CHIEF INFORMATION OFFICER.

The DoD Chief Information Officer coordinates with the DOT&E, the USD(R&E), the USD(A&S), and the USD(I&S) to synchronize the OT&E and LFT&E processes in this issuance with the:

(1) DoD Cybersecurity Program in accordance with DoDI 8500.01.

(2) DoD Strategic Cybersecurity Program pursuant to Section 1712 of Public Law 116-283.

2.6. CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

The Chief Digital and Artificial Intelligence Officer:

a. Establishes policy and issues guidance on definitions of requirements and testability for AI-enabled systems to implement and demonstrate adherence to the DoD AI Ethical Principles established in the February 21, 2020 Secretary of Defense Memorandum and the DoD Responsible AI Strategy and Implementation Pathway.

b. Issues guidance, methodologies, and best practices on T&E for AI capabilities in DoD systems.

c. Coordinates with the USD(R&E) and the DOT&E on developing and using common tools and infrastructure for T&E and verification and validation (V&V) of AI capabilities in DoD systems.

2.7. DOD COMPONENT HEADS.

The DoD Component heads follow the procedures outlined in this issuance through:

a. Component acquisition executives.

b. Program managers.

c. LFT&E organizations.

d. Their designated operational test agency (OTA) or operational test organization (referred to in this issuance as “OTA”).

SECTION 3: REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY TESTING OVERVIEW

3.1. SCIENCE- AND TECHNOLOGY-BASED REALISTIC, FULL SPECTRUM SURVIVABILITY AND LETHALITY TESTING.

a. The planning, execution, and reporting of realistic full spectrum survivability and lethality testing will be based on the latest advances in science and technology to:

(1) Determine the full spectrum survivability and lethality, as applicable, of DoD systems, in contested, congested, and constrained operational environments, including the effect of full spectrum survivability and lethality effects on operational effectiveness, suitability, and collateral damage, as applicable, with scientific rigor as the DoD system matures and adapts over time.

(2) Plan and execute risk-based level of test assessments and mission-based risk assessments (MBRAs) required to inform the scope and focus of realistic, full spectrum survivability and lethality testing.

(3) Optimize the use of data from multiple data sources, such as contractor test and evaluation (CT&E), DT&E, integrated T&E, OT&E, and LFT&E data, and M&S results, conducted on sub-components, components, sub-systems, prototypes, full-up systems, and systems-of-systems to evaluate the operational environment thresholds at which systems will be able to operate at a stated likelihood of success in support of user mission threads.

(4) Enable timely and dynamic evaluation of changes in full spectrum survivability and lethality of DoD systems throughout their operations and sustainment due to advances in adversary kinetic and non-kinetic threats and targets, and tactics, techniques, and procedures (TTP).

(5) Enable full spectrum survivability and lethality evaluation in multi-domain operations against combined kinetic and non-kinetic threat effects and targets.

(6) Identify the operational environment thresholds at which the DoD systems will be able to operate in support of user mission threads.

b. Realistic full spectrum survivability and lethality testing will use the latest available Intelligence Community knowledge and artifacts.

3.2. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY TESTING ACROSS THE ACQUISITION LIFE CYCLE.

a. The planning, execution, analysis and reporting of realistic full spectrum survivability and lethality across the acquisition life cycle will:

(1) Use data from CT&E, DT&E, and integrated T&E events (e.g., security verification, signature measurements, compliance testing, military standards).

(2) Use data and results from OT&E events (e.g., adversarial tests, countermeasure tests, hardware-in-the-loop tests).

(3) Include dedicated LFT&E events using live kinetic and non-kinetic adversary threats against DoD systems.

(4) As applicable, include dedicated LFT&E events using live employment of DoD offensive systems against adversary kinetic (i.e., physical) and non-kinetic (i.e., functional, information) targets.

(5) Use M&S results, as appropriate.

(6) Use data and results from major command or Combatant Command exercises or flag events, as appropriate.

(7) Use other T&E events, as appropriate.

(8) Identify the process by which full spectrum survivability and lethality of the DoD system will be re-evaluated throughout the operations and sustainment phase of the DoD system, as both the DoD system and the threats evolve.

b. The complexity and objectives of realistic full spectrum survivability and lethality test events will evolve as the DoD system matures across the acquisition life cycle.

(1) The T&E Working-level Integrated Product Team (WIPT), also known as the integrated test team (ITT) (referred to in this issuance as "T&E WIPT/ITT") must establish a full spectrum survivability and lethality sub-group/working group (WG) (referred to in this issuance as "LFT&E WG") to plan and execute the risk-based level of test assessments and MBRAs needed to inform the scope and focus of realistic full spectrum survivability and lethality testing, program requirements, and acquisition contracts.

(2) Realistic full spectrum survivability and lethality testing will be conducted on prioritized sub-components, components, sub-systems, prototypes, full-up systems, and systems-of-systems using cooperative tests (e.g., exploitation tests, penetration tests, controlled damage tests, recoverability tests,) and adversarial tests (e.g., operational tests).

(3) The TEMP/T&E strategy and its integrated decision support key (IDSK) will identify the live data and M&S results needed to support the full spectrum survivability and lethality

learning campaign (sometimes referred to as "building block" approach) in support of acquisition and program decisions.

c. As the DoD system matures across the acquisition life cycle and as the operational realism of test conditions increases, realistic full spectrum survivability and lethality testing in support of acquisition and program decisions will:

(1) Address any changes identified by updated MBRAs (e.g., changes to the operational mission performance requirements, new threats and threat attack vectors, updated TTP, program-initiated system modifications, system baseline upgrades including recurring software releases).

(2) Verify remediation and mitigation efforts.

d. Table 1 lists the full spectrum survivability and lethality activities across the acquisition life cycle.

Table 1. Full Spectrum Survivability and Lethality Activities

Activity		Repeated for Acquisition Decisions?
1.	Establish the LFT&E WG.	No
2.	Inform full spectrum survivability and lethality program requirements, requests for proposals, and acquisition contracts.	Pathway Dependent
3.	Conduct a risk-based level of test assessment and MBRA.	Yes
4.	Develop a full spectrum survivability and lethality T&E concept.	No
5.	Develop input to the TEMP/T&E strategy.	Yes
6.	Plan resources and schedule Federal Government testing.	Yes
7.	Review contractor development and test environment, processes, and tools.	Pathway Dependent
8.	Analyze existing or known susceptibilities and vulnerabilities.	Yes
9.	Review contractor full spectrum survivability and lethality T&E strategy and contractor test plans and data as received.	Pathway Dependent
10.	Conduct software security verification throughout the life cycle.	Yes
11.	Conduct cooperative testing.	Yes
12.	Conduct lethality testing, as applicable.	Yes
13.	Conduct regression test events.	Yes
14.	Conduct adversarial test events.	Pathway Dependent
15.	Review full spectrum survivability and lethality test results to track identified deficiencies and vulnerabilities, review plans for remediation and regression testing, and recommend mitigation strategies.	Yes
16.	For the cyber threat and target testing, incorporate test results into cybersecurity program documentation, specifically the security assessment report, risk assessment report, and plan of action and milestones.	Yes
17.	Report on preliminary or final full spectrum survivability and lethality evaluation including test adequacy.	Yes

3.3. OT&E.

a. OTAs must evaluate the effect of full spectrum survivability and lethality, as applicable, on operational effectiveness and suitability of DoD systems with trained operators, including cyber defenders, in operationally representative, contested, congested, and constrained environments.

b. OTAs will use applicable, planned OT&E events to collect the live data (as outlined in Paragraph 3.8. of DoDI 5000.98) and generate M&S results (as outlined in Paragraph 3.6. of DoDI 5000.98) required to inform full spectrum survivability and lethality evaluation including but not limited to:

(1) Susceptibility of the DoD system to kinetic and non-kinetic attacks (also referred to as "prevent"). Examples include evaluation of:

(a) Situational awareness (e.g., capability of the users, maintainers, defenders, and relevant systems, as appropriate, to detect, identify, and respond to the threat).

(b) Capability of the DoD system or users to avoid being engaged (e.g., signature control, effectiveness of electromagnetic protection (EP) and electromagnetic attack (EA), deception, expendables, the ability of the assigned cybersecurity service provider or local defender to prevent the threat from degrading or destroying the DoD system, TTP).

(2) Identification of exposures and vulnerabilities in the DoD system design and TTP in the end-to-end execution of mission scenarios including the system and the interrelated systems needed to employ and support the system. Vulnerability testing also includes the evaluation of the capabilities of the users, maintainers, and defenders to mitigate the effect of the identified vulnerability (also referred to as "mitigate").

(3) Recoverability from kinetic and non-kinetic attacks both during the operational mission and after it, including incident response plans and the capabilities of the operators and maintainers to recover from the attack, as applicable. Recoverability testing (also referred to as "recover") includes the ability of the DoD system or the user to adapt to and mitigate such effects in the future.

(4) Lethality, including the number of required weapons needed to achieve the desired lethal effects, by firing from the host platform or user production- or fielding-representative offensive capabilities against the kinetic or non-kinetic target that is operationally representative of the class of adversary systems the weapon is required to defeat, destroy, degrade, or deny.

(a) For offensive cyber capabilities, lethality testing includes exploitation of the adversary cyberspace to impose the required effects on the adversary system and its supported mission.

(b) For offensive EMS capabilities, lethality testing includes the ability to combine sensor and EA capabilities from multiple platforms to create the required and synergistic effects on the enemy system and its supported mission.

c. OTAs will use the live data and M&S results collected in LFT&E events and the planned OT&E events outlined in DoDI 5000.98 to collect the live data and M&S results required to evaluate the operational effectiveness and suitability of DoD systems in the context of full spectrum survivability and lethality effects. OTAs will:

(1) Use known and newly discovered exposures or vulnerabilities to attempt to degrade critical mission functions while the users are conducting missions.

(2) Observe and evaluate the results of the users', maintainers', and defenders' actions in a maintainability demonstration as part of an incident response scenario, including recoverability and continuity of operations, through full restoration of the affected system.

d. For OT&E events, the OTA will generate a detailed plan and a report. When applicable, within these events, the OTA will:

(1) Confirm each event incorporates the system-of-systems together with operationally representative information flows, production- or fielding-representative configurations, operational users, and an operationally representative environment.

(2) Represent the adversaries' most likely and most dangerous validated courses of action including:

(a) A DoD Cyber Red Team meeting the requirements of DoDI 8585.01 to represent contested cyberspace and coordinate and support OT&E planning, execution, and reporting.

(b) Cyber defenders.

(c) Capabilities and densities of the kinetic threat laydown.

(d) Contested, congested, and constrained electromagnetic (EM) operational environment including representative capabilities of directed energy weapons (i.e., high energy lasers and high-power microwave) and doctrinally appropriate force structures to evaluate congested and constrained environments.

(e) Chemical and biological agents.

(f) Radiological and nuclear threat effects.

(g) Threats to space-based DoD systems that the DoD system depends on for operational effectiveness, suitability, survivability, and lethality.

(h) Other operationally relevant and representative threats including but not limited to AI-based threats and data storage targets.

3.4. LFT&E.

a. The T&E WIPT/ITT will establish the LFT&E WG, which is comprised of LFT&E organizations that are responsible for following the procedures outlined in Paragraph 3.4. of DoDI 5000.98.

b. LFT&E will start in the initial stages of DoD system development at the sub-component, component, sub-system, and prototype levels and will continue with testing of early DoD system configurations, production- or fielding-representative (also referred to as full-up system-level (FUSL)), and system-of-system levels to:

(1) Identify and ensure the collection of the live data and M&S results required to inform the susceptibility evaluation. Examples include, but are not limited to, situational awareness, threat or intrusion detection, signature control, EP and EA, deception (e.g., decoys, honeypots), expendables (e.g., countermeasures), threat suppression including offensive weapons, and the ability of a DoD system or cybersecurity service provider or local defender to prevent a threat from degrading or destroying the DoD system. Susceptibility evaluation is critical to informing vulnerability testing and engagement conditions.

(2) Identify, manage, and propose mitigation to DoD system design vulnerabilities to live kinetic and non-kinetic threat effects at the sub-component, component, sub-system, prototype, production- or fielding-representative (FUSL), and system-of-system level. This includes:

(a) Cooperative testing to circumvent or defeat the security features and other vulnerability reduction features of a DoD system and identify mission critical vulnerabilities under specific conditions defined by the DoD system or mission owner and the testers. Examples include, but are not limited to, penetration, exploitation, controlled damage, EM compatibility, EM interference, EM vulnerability, EM congestion, component or material chemical or biological agent, blast, shock, and overpressure testing, including testing to evaluate second or third order cascading effects. It may include coordinated attacks.

(b) Adversarial testing to identify and assess DoD system and system-of-systems level mission critical vulnerabilities in the presence of emulated adversaries and capabilities while the unit equipped with the system is executing the required mission. It may include live and coordinated attacks.

(3) Evaluate force protection capabilities and identify user casualties, including the number, type, and severity of injury using the abbreviated injury scale. Include the evaluation of crashworthiness, as applicable, egress capability post-attack and the effect of user casualties on operational effectiveness.

(4) Evaluate battle damage assessment, repair, and recovery procedures, and the time it takes to repair or restore the damaged DoD systems and resume the mission, if any.

(5) Collect the live data and M&S results required to support the evaluation of the effect of the susceptibility, identified vulnerabilities, user casualties, and recoverability on operational effectiveness, suitability, and collateral damage.

(6) Evaluate the mechanisms required to achieve the effect of either DoD or adversary offensive systems to deny, degrade, disrupt, deceive, destroy, exploit, or influence the kinetic and non-kinetic targets. For example:

(a) Kinetic: penetration (e.g., projectile, fragmentation), shock, blast, and fire.

(b) Cyber: deny, degrade, disrupt, deceive, destroy, exploit, or influence, including cascading effects in the physical domains.

(c) EMS including directed energy: deny, degrade, disrupt, deceive, destroy, exploit, or influence, including cascading effects in the physical domains

(d) CBRN: chemical and biological agents or radioactive particles, EM pulse, blast, and thermal energy (nuclear events).

(e) Collateral effects.

3.5. M&S.

Accredited M&S may be used to deliver the results for record needed to enable and augment the evaluation of full spectrum survivability and full spectrum lethality of DoD systems. M&S used to support the evaluation of full spectrum survivability and lethality evaluations in lieu of live tests will be verified, validated, and accredited in accordance with the DoD Manual (DoDM) 5000.102.

3.6. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALIY TESTING MANAGEMENT.

a. Program Manager.

The program manager must follow the responsibilities outlined in Paragraph 3.7.a. of DoDI 5000.98 and must:

(1) Establish the LFT&E WG, M&S WG, Threat WG, and other groups, as appropriate.

(2) Ensure that the LFT&E WG is included in the development of the TEMP/T&E strategy, acquisition strategy, technical and operational requirements, requests for proposals, acquisition contracts, and related products.

(3) Ensure the availability of realistic full spectrum survivability and lethality testing resources and an executable schedule across the acquisition life cycle, including:

(a) The planning and execution of risk-based level of test assessments, MBRAs, and full spectrum survivability and lethality testing.

(b) Remediation of findings and retesting.

(c) Disposable test articles needed to support destructive testing of critical assets.

(d) Operationally representative integrated or interfacing systems for the program's full spectrum survivability and lethality test events, whether as part of the system under test or system supporting test.

(e) Threat category-specific test ranges (e.g., cyber test range) to plan, schedule, and employ T&E range infrastructure, as appropriate, during program acquisition and testing.

(f) Test assets, including their digital representations, to allow for full spectrum survivability and lethality testing throughout operations and sustainment. Maintain operational configuration information to enable reconfiguring test venues throughout the life cycle of the program to allow for live testing and to train operators on DoD system responses to cyberspace and other attacks, as applicable.

(g) Red Teams required to support realistic full spectrum survivability and lethality testing in contested cyberspace. Red Teams must be certified by the National Security Agency if testing is planned and executed on the DoD information networks.

(h) Military service-certified EMS teams required to support realistic full spectrum survivability and lethality testing in contested, congested, and constrained EM operations.

(4) Provide cyber survivability live data and M&S results to authorizing officials for use in gaining and maintaining an authority to operate.

(5) Ensure full spectrum survivability and lethality live data and M&S results are included in the data management plan.

b. LFT&E WG.

In support of the T&E WIPT/ITTs, the LFT&E WG must:

(1) Include OTA representatives, users, and subject matter experts in kinetic and non-kinetic threat effects including multi-domain operations. Examples include, but are not limited to, experts in kinetic threat effects, cyber effects (including, but not limited to, non-enterprise systems), EMS effects, EM environments, CBRN, AI-based threats, and other expertise as appropriate. Given the unique effects associated with kinetic and non-kinetic threats, the LFT&E WG may include additional sub-groups focused on detailed planning, execution, analysis, and reporting of kinetic or non-kinetic category effects (e.g., cyber WG, EMS WG, kinetic threats WG, CBRN WG).

(2) Plan, execute, and report on a risk-based level of test assessments and MBRAs to inform a defensible scope of full spectrum survivability and lethality testing while considering the operationally relevant terrain, climate, vegetation, and opposing forces that may be equipped with kinetic and non-kinetic offensive capabilities.

(3) Inform the development of program requirements related to full spectrum survivability and lethality.

(4) Provide realistic full spectrum survivability and lethality OT&E and LFT&E input to the development of the TEMP/T&E strategy including the IDSK.

(5) Define realistic full spectrum survivability and lethality testing requirements to inform requests for proposals and acquisition contracts intended to secure access to contractor-generated data, system artifacts, support, resources, and skills.

(6) Request support from, and collaborate with, the appropriate intelligence organization to conduct DoD system threat analyses, develop threat test artifacts, and identify criteria for threat surrogate accreditations.

(7) Provide required government full spectrum survivability and lethality test tool recommendations to the program manager and lead OTA and LFT&E organizations for development, procurement, and authorization to support the planned full spectrum survivability and lethality testing.

c. OTA.

The OTA(s) must follow the responsibilities outlined in Paragraph 3.7.c. of DoDI 5000.98.

d. LFT&E Organizations.

The LFT&E organizations must follow the responsibilities outlined in Paragraph 3.7.d. of DoDI 5000.98.

3.7. DATA MANAGEMENT.

Full spectrum survivability and lethality live data, M&S results, and related artifacts must be visible, accessible, understandable, linked, trusted, interoperable, secure, and managed in accordance with Paragraph 3.8. of DoDI 5000.98.

3.8. DOT&E OVERSIGHT.

a. The DOT&E must review and approve the TEMPs/T&E strategies and OT&E and LFT&E plans for programs on the T&E Oversight List for OT&E and LFT&E. This includes:

(1) Testing of the sub-component, component, and sub-system approved at the action officer and deputy director level.

(2) Early DoD system configurations, FUSL, and system-of-system level testing approved by the DOT&E.

b. OTAs and LFT&E organizations must coordinate draft plans with DOT&E staff early and often and must submit the final product for DOT&E review and approval no later than 30 calendar days prior to the start of the test, accreditation event, or M&S runs for record.

c. The program office, OTA, and LFT&E organizations must coordinate draft M&S V&V plans and accreditation plans with DOT&E staff early and often and must submit the final products to the DOT&E for review with sufficient time to influence M&S validation, verification, and accreditation decisions.

d. The DOT&E must review and provide a decision on concurrence on T&E concepts for LFT&E. LFT&E WG must deliver the T&E concepts to the DOT&E early enough to support the planning and execution of integrated T&E, OT&E, and LFT&E.

SECTION 4: REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY TEST PROCESS

4.1. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY TEST PLANNING.

a. Overall Planning Concepts.

(1) T&E WIPT/ITT and its LFT&E WG, in conjunction with the OTA and LFT&E organizations, will plan realistic full spectrum survivability and lethality testing in support of acquisition and program decisions in accordance with DoDI 5000.98 and DoDM 5000.100.

(2) The planning will include the risk-based level of test assessment, the MBRA that will consider prior live test or combat data, and other information and factors that may affect the full spectrum survivability and lethality evaluation.

(3) For each kinetic and non-kinetic threat category, the realistic full spectrum survivability planning must support the evaluation of the survivability kill chain including:

(a) Susceptibility to an adversarial engagement.

(b) Vulnerability to kinetic and non-kinetic threats, if engaged, including the evaluation of the effect of the vulnerability on operational effectiveness and suitability.

(c) Recoverability during or after the engagement and while conducting the mission or after the mission.

(d) User casualties and egress abilities, as applicable.

(e) Coordinated kinetic and non-kinetic threat engagements' effect(s) on operational effectiveness, suitability, survivability, and lethality, as applicable.

(4) For offensive DoD systems, realistic full spectrum lethality planning must include the evaluation of the adversarial kill chain including:

(a) The specific characteristics of the lethal mechanism or effect (e.g., warhead characterization, penetration, deny, degrade, disrupt, deceive, destroy, exploit, and influence capabilities).

(b) Lethality as fired or deployed from the host platform or by the user against operationally relevant and representative targets.

(c) The effect of adversary susceptibility on DoD offensive capability lethal effects (e.g., adversary countermeasures, defenses, TTP).

(d) The effect of an offensive attack on collateral damage.

b. Input to the TEMP/T&E Strategy.

(1) The T&E WIPT/ITT must include full spectrum survivability and lethality OT&E and LFT&E requirements in the TEMP/T&E strategy, including its IDSK, in accordance with DoDI 5000.98 and DoDM 5000.100.

(2) The development of the TEMP/T&E strategy and its updates will build upon all relevant live data and M&S results conducted at the sub-component, component, sub-system, prototype level, and on early DoD system configurations to reduce risk to and optimize of, fielding- or production-representative FUSL and system-of-system levels. This building block approach will support the full spectrum survivability and lethality learning campaign as the DoD system matures across the acquisition life cycle.

(3) The TEMP/T&E strategy updates must include an updated risk-based level of test assessment and MBRA to account for the latest threat, attack surface analysis, and improved understanding of mission critical functions and potential vulnerabilities.

c. Realistic Full Spectrum Survivability and Lethality Test Plans.

(1) LFT&E organizations must design realistic full spectrum survivability and lethality test plans in accordance with DoDI 5000.98 and the approved TEMP/T&E strategy.

(2) Test plans will be required for:

(a) Cooperative tests using live kinetic and non-kinetic threats to identify mission critical vulnerabilities at the prioritized sub-component, component, sub-system, system, FUSL, and system-of-system level and their effect on operational effectiveness, suitability, recoverability, and user casualties. A separate test plan may be required for each threat category (e.g., kinetic threats, cyber, EMS including directed energy, CBRN). A waiver from FUSL testing may be granted in accordance with the procedures in accordance with Paragraph 3.4.g. of DoDI 5000.98.

(b) Adversarial tests to evaluate early DoD system configurations, fielding- or operationally representative, and system-of-systems mission critical vulnerabilities and their effect on operational effectiveness, suitability, recoverability, and user casualties in the presence of emulated adversaries and adversarial capabilities. Such tests must be included as part of integrated T&E and OT&E.

(c) Measurement and evaluation of susceptibility, including any susceptibility reduction features for each threat category. Aspects of susceptibility testing may be included as part of integrated T&E and OT&E.

(d) Characterization of the offensive capability and its lethal effects on operationally representative materials, sub-components, components, sub-systems, full-up systems, and system-of-systems.

(e) End-to-end offensive capability lethality testing in contested, congested, and constrained operationally representative environments against operationally representative

kinetic and non-kinetic targets (or accredited surrogates). Such tests may be included as part of integrated T&E and OT&E events.

(3) Separate test plans may be required for recoverability testing depending on the complexity of the DoD system (e.g., recoverability of the ship after a kinetic threat attack).

(4) See Table 2 in Appendix 4A for the types of data or information needed in either cooperative or adversarial test plans. Security verification tests and automated software assurance scripts do not require a test plan.

d. MBRA.

(1) The T&E WIPT/ITT must plan and execute the MBRA to inform a defensible scope of relevant OT&E and LFT&E and prioritize the full spectrum survivability and lethality testing of sub-components, components, sub-systems, systems, and systems-of-systems.

(2) The MBRA must assess potential vulnerabilities and risks to mission critical functions, components, and interfaces in the contested, congested, and constrained operational environment based on the:

(a) Detailed mission and operating environment description and decomposition including a mission criticality analysis. Example unique to the MBRA for EMS include, but are not limited to:

1. Friendly forces, neutral actors, and adversary forces with active emitters used for military, civilian, or government purposes.

2. Frequencies, bandwidths, operational modes, polarization, waveform type, and transmit and receive power levels for each of the stationary or moving emitters for the force structure derived from the concept of operations or other requirements document.

3. The location of the stationary or moving emitters and how their impact on the EM operational environment could change during the mission based on a scenario laydown.

(b) Detailed DoD system description and DoD system functional decomposition, including, but not limited to, the DoD system's mission critical functions, architectures, software, hardware, data flows, interfaces, protections, maintenance processes, and a list and analysis of existing or known vulnerabilities that includes the software factory and bill of materials, as applicable.

1. DoD system descriptions include detailed characterization of the attack surface for non-kinetic threats and relevant DoD system architectures and program artifacts to identify relevant forms of communication, network connectivity, software, hardware, supply chain, and human interaction that could be vulnerable to non-kinetic threat effects.

2. See Table 3 in Appendix 4A for examples of evolving attack surface elements.

(c) DoD system-relevant intelligence product(s) including current and emerging threat characterization. The MBRA should consider categories or families of threats when detailed information on specific threat systems is not available.

(d) Characterization of the survivability kill chain to evaluate mission critical kinetic threat engagement conditions and non-kinetic attack vectors.

(e) Input from operational users, defenders, maintainers, developers, and engineers.

(3) The MBRA:

(a) Must be updated at each acquisition decision and throughout the DoD system's operations and sustainment as the threat, DoD system, operational environment, or mission evolve.

(b) Must include all threat category relevant to the system's concept of operations to evaluate unique threat effects on attack vectors or engagement conditions and threat effects on mission critical functions.

(c) Output must detail the attack scenarios with recommendations for remedies, mitigations, and testing.

(4) Live data and M&S results will validate MBRA results.

e. Realistic Full Spectrum Survivability and Lethality Test Input to Contract Requirements.

The T&E WIPT/ITT will advise the program manager in structuring acquisition contracts to include the information required to support realistic, full spectrum survivability and lethality evaluation. Examples of required information include, but are not limited to:

(1) Relevant contractor's full spectrum survivability and lethality test plans before testing begins and any resultant live data, M&S results, and reports.

(2) Inclusion of T&E WIPT/ITT as observers of contractor full spectrum survivability and lethality T&E events and design reviews.

(3) Physical access to relevant contractor facilities, system integration laboratories, systems developmental networks, environments, cloud infrastructure, and supplier software development environments.

(4) Access to DoD system artifacts including, but not limited to, design details such as components, functions, fault tree or equivalent analysis, digital representation of the DoD system, supply chain information, source codes, and other information needed to plan and execute the MBRA and relevant M&S.

(5) Contractor's mitigation or remediation responsibilities.

(6) Development of test articles and DoD system surrogates or digital representations, if not available.

f. Input to Program Requirements.

The T&E WIPT/ITT must evaluate, inform, and report on full spectrum survivability and lethality requirements to identify weak or missing requirements and assess their testability so they can be evaluated with statistical confidence. The program manager must use these findings to write contract language, synchronize and deconflict requirements, and ensure the DoD system is hardened against full spectrum threats and imparts the required lethal effects in contested, congested, and constrained operational environments, as applicable.

4.2. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY TEST PREPARATION AND EXECUTION.

The OTA and LFT&E organizations must prepare and execute the cooperative and adversarial tests in accordance with the procedures outlined in Paragraphs 4.2. and 4.3. of DoDI 5000.98 and approved test plans. Test preparation and execution will:

a. Confirm the test tools, test facilities, required test instrumentation, data collection plan, test asset, interfaces, infrastructure, defenders, embedded support contractors, trusted agents, and permissions are available.

b. Ensure the test tools do no unintended harm to the DoD system under test unless the planned test asset or environment supports a destructive test event.

c. For cyber tests, allow the test team's freedom of exploration to collect discovery learning insights, unless affected by safety, law, regulation, or other limitations as defined in the test plans.

d. For spectrum tests, allow the test team freedom to build representative operational EMS environments through live, virtual, or constructive environments for realistic full spectrum survivability and lethality test preparation and execution.

e. For EMS-dependent systems, collect data that characterizes the technical characteristics of the receiver, transmitter, and antenna spectrum dependent devices as well as the technical characteristics of the waveforms generated.

4.3. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY ANALYSIS AND EVALUATION.

Test organizations must follow the procedures outlined in Paragraph 4.4. of DoDI 5000.98 to support rigorous full spectrum survivability and lethality analysis.

4.4. REALISTIC FULL SPECTRUM SURVIVABILITY AND LETHALITY REPORTING.

a. The OTA and LFT&E organization must report on full spectrum survivability and lethality in accordance with the procedures outlined in Paragraph 4.5. of DoDI 5000.98.

(1) OTAs must:

(a) Provide full spectrum survivability and lethality data collected during integrated T&E and OT&E events in support of the full spectrum survivability and lethality input to the report.

(b) Consolidate inputs from LFT&E organizations to report on the effect of full spectrum survivability and lethality, as applicable, on operational effectiveness and suitability.

(2) LFT&E organizations must:

(a) Report on full spectrum survivability and lethality evaluation, as applicable, using the data collected during CT&E, DT&E, integrated T&E, OT&E, and LFT&E events.

(b) Support the OTA's report with full spectrum survivability and lethality evaluation.

b. Full spectrum survivability and lethality input to consolidated DoD system reports must include the baseline information outlined in Table 4 in Appendix 4A.

APPENDIX 4A: DETAILED FULL SPECTRUM SURVIVABILITY AND LETHALITY PLANNING AND REPORTING REQUIREMENTS

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data

Topic	Description
System Description and Requirements	• Describe or provide a reference or a digital representation of the DoD system and the system-of-systems with focus on design features that will affect full spectrum survivability and lethality testing and scope. Examples include: **Survivability** – Survivability enhancement features including any design features or equipment intended to reduce the DoD system's: ▪ Susceptibility (e.g., situational awareness, intrusion detection, signature control, EP and EA, deception (decoys, honeypots), expendables, threat suppression and offensive weapons). ▪ Vulnerability (e.g., component location and logical separation, component and system redundancy (with effective separation and diversity), passive and active damage and malfunction suppression through hardening (e.g., shock hardening, coating, cybersecurity hardening such as host-based security system, antivirus), component and system capability recovery, component shielding). – Major components, sub-systems, and their interfaces to other components, systems, networks, systems-of-systems (e.g., maintenance laptops, support equipment, servers, the cloud, virtual computers, and software appliances), and systems on which the DoD system depends (e.g., support equipment). – The operational network including actual configurations, addresses, and data flows (e.g., ports, protocols, and services for each address). – Major DoD system functions that could be affected by their damage or malfunction including fault trees. – Internal interconnections between major sub-systems (e.g., data bus links, any features which may function as wave guides). – Internal networks (e.g., local area networks), configurations, connections, and data flows. – Physical access points (e.g., universal serial bus ports, drives, peripherals, and other media). For contractor-owned facilities, programs should pre-negotiate physical access points in the contract. – Specific versions and configurations of testable DoD system modules including hardware, software, and firmware that are part of the DoD system, using the software and hardware bills of material. – DoD system's reliance on EMS and EMS interfaces to other components or systems. Include the technical characteristics (e.g., DD Form 1494 data) of EMS-dependent devices such as the operational transmit and receive bands or specific operational frequencies, transmit power, and receive sensitivities. ▪ For antennas, include the antenna pattern across the frequency and modes of operations and polarization. ▪ For transmitters, include the transmit power and waveforms capable of being produced. ▪ For receivers, include the receiver sensitivities, selectivity, and saturation points. ▪ Describe the EA techniques (e.g., waveforms) that can be generated, along with the created effects and the threshold of operation at the receiver (e.g., jam-to-signal ratio, persistence time), that can be mitigated by the EP techniques along with the threshold (e.g., jam-to-signal ratio) at which this mitigation occurs. – System parts or components that will require supply chain risk analysis.

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
System Description and Requirements	– Description of development, test, or production environment and processes and tools included as part of the DoD system (e.g., software factory, test equipment, manufacturing line). – If applicable, describe targeted forensic images of the DoD system-like defender workstations, including operational configurations and tools. **Lethality** – Warhead and fuse design. – Cyber exploits relevant to DoD system architecture, DoD systems, applications, hardware, networks, and bus protocols. – EA techniques, EP techniques that can mitigate the EA techniques and the threshold (e.g., jam-to-signal ratio) at which this mitigation occurs. – Characterization of the laser systems to include beamwidth, jitter, wavelength of operation, waveform characteristics (e.g., continuous wave, pulse parameters, pulse train parameters), polarization, power beam, and beam director details (e.g., trackers, aimpoint maintenance), power and thermal sub-system including energy generation and storage requirements, maximum continuous single firing duration, firing duty cycles. – High power microwave power output, frequency, bandwidth, pulse width, cycle, repetition.
Test Environment	• Describe the kill web, mission thread, or mission scenarios that will be represented in the test, including timelines, spatial constraints, and state or mode of operation. • Describe the test conditions including similarities and differences between the test environment and the operational environment defined by the Intelligence Community, as applicable: – Availability of all operationally representative components critical to the evaluation objectives. – Contested, congested, and constrained EM operational environment unique to the specific mission thread and region that considers friendly, neutral, commercial, and adversarial systems in the environment. Include spectral characteristics (e.g., emitter frequencies, modulation, bandwidths, operational modes, transmit and receive power levels). See Joint Publication 3-85 and DoDI 4650.01 for details. – Threats and effects used in tests and risks exposed by the MBRA. – Locations, configurations, and management of anticipated sensors and data collection instrumentation. – Information for coordinated mission frequency planning and allocation. – Atmospheric and environmental conditions that could affect the threat effects. Examples include optical turbulence and aerosols or particles along the high energy beam path to estimate the time required to engage each target, noise, vibration, acceleration, shock, acoustic, EMS emissions, and other environmental factors, particularly for airborne or shipborne tests. – Integrate high power microwave testing with electromagnetic warfare testing. • Describe any assumptions and limitations that may affect the test conduct along with proposed mitigations. Examples include: – Frequency constraints and limitations in amplitude to prevent interference or damage to local electronic and communications infrastructure. – Security or safety risks including any resultant rules of engagement and simulated aspects of test. – Use of M&S (e.g., system integration lab, hardware integration lab). • Condition of the test article under test as compared to its operationally representative properties.

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
Time and Resources	• Provide the schedule of test events and resources. Examples include: – Dates, facilities, and locations for the testing. – Expendable and non-expendable test assets. – Locations and anticipated roles and responsibilities for test stakeholders including, but not limited to, tiered and end users, operators, DoD system or network administrators, cybersecurity service providers, defensive cyberspace operators, maintenance teams, and data collection support teams. – Test and data collection tools, automated or otherwise. – Other test resources and security agreements (e.g., interconnection security agreement) for support of ranges, services, operational data and exchanges, hosting systems, simulations, or specific test equipment. – Roles and responsibilities to return the DoD system to a usable state. • Describe any authorizations required to conduct the test (e.g., authorization to operate, interim authorization to test, hosting system agreements, directed energy weapon and EMS authorizations). • Describe verification, validation, and accreditation status for models, simulations, tools, labs, and any other component of the test environment. For V&V plans, follow the procedures outlined in DoDM 5000.102. • State format of data with intended recipient(s). • Provide the date for full and prompt access to the data, in accordance with the data management plan.
Vulnerability Tracking and Retesting	• Describe the process to document, track, and determine severity of vulnerabilities during the test. • Describe requirements needing retest. • Identify fixes, TTP, and mitigations to previously identified vulnerabilities and exposures needing confirmation through testing. • Use prior approved test plan for regression testing.
All Test Activities	• Describe how the test team will conduct the test activities and gather required data. • Describe the threats and targets, as applicable, that the team will portray including their validation and accreditation, as applicable. For each planned attack technique or engagement, list the attack or engagement conditions and operational objectives. Describe the attack surface, DoD system vulnerabilities, including EMS system spectrum vulnerabilities, and any changes to the attack surface exposed by the mission. • Describe any automated or manual tools used for the test, including cyber tools, their versions, the team's standard operating procedures, and rules of engagement. • Describe any plans to employ sensors or other monitoring functions to collect the test results. Specify all other test and data collection methods and tools, which may include the following: – Direct or indirect measurements (e.g., EMS sensors). – Hardware-in-the-loop. – M&S. – Built-in test or logging. – Physical inspection. – Personnel interviews. – Log review, ruleset review, DoD system configuration review, and file integrity checking. – Artifact reviews. – Data collection forms and other documents.

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
Susceptibility Test Activities	• Describe the purpose of susceptibility tests either as standalone tests or as part of an integrated OT&E, LFT&E test and explain what data and M&S results will be collected to evaluate, with confidence, the following: – Situational awareness of kinetic and non-kinetic threats (e.g., radar warning receiver, abnormal operation reports, missile warning sensors, chemical or biological threat detectors). Describe how during or after an attack the test will collect the observations and actions of the operators and the defenders (e.g., defender logs, system logs) and assess the defenders' knowledge in advance of the attacks. – Signature and signature management (e.g., radar cross section, EM emissions, low observability technology, air gaps). – Defensive capabilities including, but not limited to, EP and EA, deception (e.g., decoys, honeypots), expendables (e.g., flares), threat suppression, and offensive weapons. • Describe the metrics and measures the test team will collect to evaluate the training of the operators and defenders intended to defend the DoD system against an attack. – Description of the expected DoD system defender defensive tools, including their versions and capabilities. – Description of how the test team will collect information on defensive tools employed by the DoD system defenders (including cybersecurity service provider, if able) in observed defender actions.
Vulnerability Test Activities	• Describe the purpose of planned cooperative and adversarial tests at the sub-component, component, sub-system, system, full-up system, and system-of-systems level testing including, but not limited to, scan tests, penetration tests, shock tests, exploitation tests, controlled damage test using live kinetic or non-kinetic threats (or simulated effects if required) to evaluate vulnerabilities in the physical space, cyberspace, and EMS. • As applicable, describe the activity to verify mitigation or correction to previously identified mission critical vulnerabilities (e.g., at the component, sub-system, DoD system levels) to determine whether the vulnerability still exists or whether DoD system changes or other factors remediated the vulnerability. • Describe the planned collection of mission performance metrics and measurements to enable assessment of the effects of the identified vulnerability on operational effectiveness and suitability. (The nomenclature and format of the data should be aligned across integrated T&E, OT&E, and LFT&E) • As applicable, describe the testing for evaluation of force protection capabilities and the effect of the observed threat effects on user casualties. – Determine the type and number of injuries and the effect of those injuries on operational effectiveness, suitability, and lethality. Use the abbreviated injury scale to classify and describe the severity of the injuries. – Determine the effect of the threat effect and user casualties on egress capabilities.
Vulnerability Test Activities – Kinetic Threats	• Describe the rationale for the number and types of test events (e.g., penetration, exploitation shots, shock tests, controlled damage events). • Describe the engagement conditions and associated rationale.

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
Vulnerability Test Activities – Cyber Threats	• Describe the techniques the test team will use in test, including any automated or manual test tools and their versions. • Describe how the test team will capture the test conduct and results (e.g., attacker logs). • Describe the initial access condition for each test. Test all initial access conditions unless they are not applicable to the DoD system under test. Identify initial access conditions based on whether the threat has logical or physical access as follows: – No physical access and no logical access. – Physical access and virtual access. – Virtual access but no physical access. • Describe how the test team will use results from prior security verification and conduct the test activities. For example: – Describe how the test team will conduct any DoD system vulnerability scans, including any employed tools, their versions, and any prerequisites (e.g., DoD system credentials). Tools may include automated system discovery scanning, vulnerability scanning, and software assurance tools. The test team will use a software bill of materials or software composition analysis of the DoD system under test to build the list of vulnerabilities to test. Tools will at a minimum scan for vulnerabilities documented in the National Vulnerability Database. – Assess exploitability of known vulnerabilities. – Describe any planned testing derived from security verification data (e.g., security scans, software assurance reports, Security Technical Implementation Guide scan results, Risk Management Framework Plan of Action and Milestones). • Describe how the test will gather attack kill chain data from the attackers and their activities (e.g., attacker logs, action maps, tool outputs). – Describe how the test will gather data to evaluate if EMS enables or hinders aggressive cyber activities. – For financial or business DoD systems, provide a defined set of economic attack scenarios from MBRAs and rules and requirements for the cyber economic vulnerability assessments testing. Describe user roles and responsibilities, procedures for monitoring alerts, and any results from pre-production scans. Document mission effects, including fraud, embezzlement, or significant economic losses resulting from cyber exploits.
Vulnerability Test Activities – EMS Threats	**Congested EMS** • Evaluate spectrum pathways in different operating environments (e.g., land-based emissions, shipboard environment). • Describe the test to identify vulnerabilities of integrated DoD systems and sub-systems in background noise EMS conditions. • Summarize outcome of electromagnetic environmental effects (E3) and spectrum management activities (e.g., DD Form 1494, Military Standard MIL-STD-461G/464D/2169D, Military Handbook MIL-HDBK-235-8, JF-12 spectrum certification process) including vulnerabilities identified during intra-platform and equipment E3 tests, EM interference, EM compatibility, EM pulse, lightning, precipitation static, laser attack, high-power microwave attack, and other relevant testing. • Describe co-site interference tests to identify any vulnerabilities introduced by colocation of antennas and other transceivers and electronics. • Describe EM compatibility victim-source test to identify vulnerabilities of the victim systems. • Describe the test to determine the maximum range at which point-to-point communications and data links are at an acceptable level to support the mission.

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
	Constrained EMS • Describe the test to evaluate the effect of constrained EM environment (e.g., civilian C-band radar overlap with NATO G-band radar frequencies) on the use of the DoD systems to minimize detection, exploitation, or other interactions (e.g., interference-based localization or active emissions during vulnerability periods to other systems). • Describe scenarios that detail operational constraints that result from either a directive to deconflict or to not conflict with or divulge operational capabilities to other users. Example of constraints include: – Timeline of potential interactions which drive on and off power constraints. – Spatial constraints (e.g., main or side lobe generation patterns, or terrain shielding). – Operating state or mode constraints, specific to both active and passive as well as electromagnetic warfare and EP techniques being used (or protected). If the power or mode of the system may cause direct harm, describe a likely use case (e.g., airborne EA GPS jamming during testing which results in denied or degraded GPS navigation for commercial airliners in the area – a public safety constraint on testing and training). **Contested EMS** • Describe adversary EA capabilities, the physical paths the adversary could use, and the EP capabilities of the DoD system under test. • Describe the scenario that includes timelines, spatial constraints, and the state of mode of operations, and: – Describe the planned collection of mission performance metrics and measurements to enable assessment of the effects of a hostile EM environment. – Describe the threats (and validation of the threat) the adversarial team will portray. For each planned EA technique, list the operational objectives (target(s) and intended type of effect). – Describe any additional hardware needed (e.g., horn antenna, pole, laser surrogate). – Describe how the test will verify attack data and activities (e.g., attacker logs). – Test the known vulnerabilities documented during E3 and related requirements testing. – Describe how the test team will collect the actions of the operators and DoD system during deployment of EP measures and minimize EM interference, during or after an attack. – Describe how the test team will evaluate performance degradation to EA. – Describe how the test team will test for DoD system response to and recovery from EA. • Describe planned EMS testing including key radio frequencies, data links, and other spectrum pathways, and how testing will support assessment of EM operations to accomplish or defend against cyber and directed energy exploitation.
Vulnerability Test Activities – CBRN Threats	• Describe the testing to evaluate the effect of the DoD system's exposure to chemical and biological agents on mission critical components, sub-systems, systems, and user casualties (where possible). Agents can degrade materials, incapacitate personnel (including, but not limited to, poisoning), and cause disease. Use actual agents when feasible and suitable simulant(s) when necessary (such as in system-level testing). • Describe the effect of radiological effects caused by nuclear fallout of dirty bombs on materials and user casualties. • Describe the effect of nuclear detonation in additional to radiological effects on equipment and user casualties including: – Blast, shock, and overpressure – analyze using structural analysis and M&S and directly measure using high explosives and shock tubes. – Thermal radiation – analyze thermal radiation effects and directly measure flash

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
	blindness shielding component. – EM energy – directly measures the EM pulse effects. See Military Standard MIL-STD-2169D. – Ionizing radiation – analyze gamma ray and neutron effects. For space systems add X-rays and electrons. Directly measure for small components (as possible). – Disturbed operating environments – assess radio frequency effects via communication or radar computer simulators, optical effects via clutter simulators, and dust effects via dust erosion facilities. • Evaluate the effectiveness of any hardening features designed to protect the DoD system against CBRN and the effectiveness of the protection gear provided to the user. • Evaluate the ability of users to conduct their mission(s) in the protective gear.
Recoverability Test Activities	• Describe how the test team will test and evaluate the ability of the user or the defender to recover from live and simulated kinetic and non-kinetic attacks. Evaluate the effectiveness of the recoverability process and the time it takes to resume the mission (either fully or partially, it at all). • Include the effect of the recoverability process and capability on operational effectiveness and suitability. • For chemical and biological threats, describe the decontamination process, including, but not limited to, the ability to suppress the chemical and biological agents to acceptable levels. Assess the effect of the decontaminant on materials and user casualties and residual performance of the DoD system after decontamination. • Include the assessment of the time frame for recoverability.
Lethality Test Activities	• Describe the tests that will include firing of the production- or fielding-representative offensive capabilities against the target that is operationally representative of the class of systems the weapon is required to defeat. • Describe the testing or analysis that will support the evaluation of the number of required weapons needed to achieve the desired effect on the target of interest. • Describe the effect of the lethal effects on collateral damage. • Describe the testing or analysis required to evaluate the effect of the adversaries' situational awareness, signature management, and defensive capabilities on the DoD system's offensive lethal effects. • Characterize the offensive capability lethal mechanism using ground, open air, or underwater tests, and M&S. **Kinetic weapons** • Include arena tests in accordance with Joint Technical Coordinating Group for Munitions Effectiveness Publications. • Include gun-fired fragment or projectile testing in laboratory tests, as applicable. • Include blast chamber overpressure tests and static tests against witness panels and range targets. • Include sled or rail tests to assess penetration capability and fusing. **Cyber offensive capabilities** • Design offensive cyber capability tests in accordance with the minimum test considerations captured in DoDI O-3600.03. **Directed energy weapons** • Include diagnostics testing to measure high energy laser: – Power levels or irradiance. – Power and spot size measurements at range and jitter. – Atmosphere characterization along the beam path (e.g., refractive index structure parameter, aerosol scattering and aerosol absorption, particulates, wind speed and direction).

Table 2. Baseline Realistic Full Spectrum Survivability and Lethality Test Plan Sections and Data, Continued

Topic	Description
	– System firing back-end capabilities (e.g., battery charge (if applicable), coolant temperatures). – Pointing accuracy. • Include testing to measure target detection, tracking, and identification capabilities: – In a representative environment including potential clutter background. – Against operationally representative targets and in accordance with the appropriate concept of operations, rules of engagement, and TTP for the directed energy weapon. – Using source of truth data source(s) for target tracking and subsequent data analysis. – Using necessary sensing and cueing systems, and command-and-control architecture. – In accordance with the Laser Clearinghouse approval for any use of above-the-horizon high energy laser.

Table 3. Examples of Evolving Attack Surface Elements

Attack Surface Elements	Actions
Additive and Computer-Aided Manufacturing	• Characterize risks associated with part integrity and data corruption.
AI, Machine Learning, and Big Data Applications	• Consider adversarial AI/data attacks (e.g., data poisoning). • Consider susceptibility of altered analytics and other attacks.
Commercial Cloud Environments and Cloud Services	• Consider access to contractor test data and conducting cyber testing of cloud service infrastructure and implementation. • Consider physical and logical components of the hosting cloud or center for hosted systems. • Consider how the cloud architecture interfaces with the DoD system and government networks. • Consider cloud Service-level agreement(s) to determine service speed and productivity, program risk exposure, and responsibilities. • Consider government-mandated data exposure for reporting and analysis for secure coding, speed of vulnerability mitigation and incident reporting found in the Department of Homeland Security's Cybersecurity and Infrastructure Protection Agency's EINSTEIN database.
Defense Industrial Base	• Characterize the risk of data exfiltration about and from the DoD system and monitor defense industrial base breaches. • Evaluate cyber supply chain risk management assessments and risk tolerance actions.
DoD Infrastructure and Enterprise Services	• Evaluate the DoD system's dependencies on and interfaces with external infrastructure and services. • Evaluate trust relationships and implementation of "Zero Trust" architectures, as applicable.
EMS	• Identify and evaluate any DoD system susceptibilities to cyberspace attacks in and through the EMS.
Inter- and Intra-System Architecture Network Interfaces	• Evaluate the dependencies on interfaces to supporting or underlying infrastructure, including U.S. critical infrastructure (e.g., power grid, water, communications, emergency services). • Evaluate (using network interfaces and technology regardless of the network including DoD networks) networks local to the DoD system, and non-Internet Protocol networks (e.g., Military Standard MIL-STD-1553C). • Evaluate the infrastructure dependencies and validate contingency planning, continuity of operations, and disaster recovery planning occurs. • Validate the adequacy of the critical infrastructure protection plan. • Evaluate the transition points from Internet Protocol to control systems' protocols for opportunities to detect intrusions.
Interfaces with Interagency	• Evaluate interface risks using cyber threat intelligence from all available government sources (e.g., Defense Intelligence Enterprise sources, Defense Intelligence Threat Library, Central Intelligence Agency, Federal Bureau of Investigation, Department of Energy, Department of Homeland Security's Cybersecurity and Infrastructure Security Agency). Commercial threat information can be used as cueing for collaboration with the Intelligence Community.

Table 3. Examples of Evolving Attack Surface Elements, Continued

Attack Surface Elements	Actions
Real-Time, Safety-Critical Systems (e.g., Industrial Control Systems, Supervisory Control and Data Acquisition)	• Develop relevant test approaches, making use of information from expert sources, such as maintainers, systems engineers. • Include mission defenders at all levels in the list of personnel supporting test approach development. • Evaluate incident response processes using the advanced cyber industrial control system TTP for DoD.
Software Factories	• Evaluate processes and tools within development pipelines, including those involved in producing and deploying software. • Evaluate the cybersecurity of the software development environment. If possible, evaluate the development environment before generating code.
Supply Chain	• Use the program MBRA for cyber to inform testing scope via fully sourced criticality, interdependence, and operational considerations. • Include contractual requirements (i.e., test procedures and resources) for supply chain testing. • Evaluate software, firmware, hardware, and bills of materials to determine provenance. • Evaluate if the DoD system and its constituents include any content from suppliers that have been suspended, debarred, or excluded from procurement. • Evaluate software and hardware assurance efforts.
System Architecture and Design Choices	• Evaluate critical functions and the proposed or anticipated architecture and implementation information (or architectural information from prototypes or surrogate systems if required) to identify relevant specified or derived requirements.

Table 4. Full Spectrum Survivability and Lethality Baseline Test Reporting Requirements

Topic	Information
Survivability	• Record and report data using the kill chain construct including the discussion of adversarial TTP for each of the threat categories. Report on the susceptibility, vulnerability, recoverability, and user casualties, as applicable, and their effect on operational effectiveness and suitability. • Record any deviations in the DoD system under test, test environment, limitations, tools, threats, M&S, and other elements, as compared to the approved test plan. • For cyber: – For each activity (successful or not), report time on keyboard, addresses, port/protocol, timeline, privilege level, tool used, target and source system, and results using Red Team Action Maps or an equivalent reporting scheme. Data should include items such as time-ordered, time-stamped command line input with attacker comments. – Provide evidence of success for successful attacks. – For successful attacks, report the specific DoD system configurations and root causes. – Report all use of simulated activities, assumptions, "white cards," and describe results and impacts associated with using the white cards. • For EMS: – Report the probability that a sensor system (e.g., signal intelligence, EMS support) will be able to detect and identify a given emitter waveform or mode of operation of a threat system. – Report the length of time it takes for a sensor system (e.g., signal intelligence, EMS support) to detect and identify a given emitter waveform or mode of operation of a threat system at various threshold levels and probabilities of correct identification and detection. – Report the length of time it takes to activate the correct EP technique when exposed to the EA technique. – Report the effects created in the system prior to and after the EP techniques are employed. – Report the effectiveness of the EP techniques against a wide variety of EA threats.

Table 4. Full Spectrum Survivability and Lethality Baseline Test Reporting Requirements, Continued

Topic	Information
Susceptibility	• Record and report data and the evaluation of situational awareness, signature and signature management, and defensive capabilities for each threat category. • For kinetic threats, report on the probability of the kinetic threat hitting the DoD system including likely hit locations, miss distances, and uncertainty quantification. • For cyber: – Describe the inherent (baseline truth) and inherited (deltas) cyber defenses state of the DoD system including hardware, software, and firmware and the accuracy of the information. – State cyber actions prevented and means of prevention (success). – State cyber actions not prevented (failures). – Quantify the number of anomalous observations, their severity and frequency – Describe detection of cyberspace attacks including the following: ▪ Organization (who/how detected/not detected). ▪ Cyber actions detected and method of detection (e.g., logs from devices active in defense). Evaluate which detections correspond to known actions and which do not (false positives). ▪ Mode of detection (automated, manual, user-reported). ▪ Monitoring tool data (name, type, and version). ▪ Detection timelines – initiation to completion. ▪ Attack indicators. ▪ Quantify the number of anomalous observations, their severity and frequency, ▪ Effectiveness of any countermeasures, as applicable. • For EMS: – Report on the effectiveness of EM support and EP (e.g., passive countermeasures) and EA to suppress the threat. – Evaluate how well the system can detect, identify, and locate threat systems in the operating environment based on analysis of the EM signature, either independently or cooperatively with other assets. – For EP techniques, report the jam-to-signal ratio and the length of time required for a given EA technique to produce detrimental effects given the EP techniques implemented by the receiver. – For EA techniques, report the jam-to-signal ratio and the length of time required for the EA technique to produce a desired effect on the receiver given the EP techniques implemented by the receiver. – For EA techniques, report the effectiveness of the EA technique and the target system effects created. • For CBRN, report on the threat detection capabilities including timelines.

Table 4. Full Spectrum Survivability and Lethality Baseline Test Reporting Requirements, Continued

Topic	Information
Vulnerability	• Describe the identified vulnerabilities for each threat category and their effect on operational effectiveness and suitability. • Provide mission or capability performance data and evaluation during and after the attack. • Identify the types and number of user injuries including the abbreviated injury scale and the effect of those on operational effectiveness and suitability. Include evaluation of egress capabilities. • For cyber: – Enumerate cyber vulnerabilities (using National Vulnerability Database/Common Vulnerability Enumeration data when available), exposures, and patching status (e.g., collated credentialed and uncredentialed vulnerability scans). – Describe each vulnerability or exposure and where found (e.g., what portions of the DoD system under test, network). Specify vulnerability or exposure score (e.g., Common Vulnerability Scoring System). – Quantify the number of anomalous observations and their severity and frequency. – Include data covering all the scanning (reconnaissance) activities (e.g., device or service logs, defender or administrator or operator logs, associated help desk tickets, system continuous monitoring tools, relevant screenshots). – List tools, versions, and settings used to complete scans. – Provide explored or discovered data in the actual operational configuration from all supply chain risks. – For exploited vulnerabilities and exposures, report the attained access. Review the exploit data to determine the detectability of the exploit or attack. – Identify means used to determine access (e.g., analyses, subject matter expert assessment, penetration test). – Identify the basis for developing potential attack vectors to explore for mission effects. – For financial or business DoD systems, document cyber economic vulnerability assessments findings. • For EMS: – Report on the effectiveness of redundancy, resiliency, and responsive actions (e.g., active countermeasures). – For EP techniques, report the jam-to-signal ratio and the length of time required for a given EA technique to produce detrimental effects given the EP techniques implemented by the receiver. – For EP techniques, report the protection effectiveness against operationally representative and relevant EA techniques.

Table 4. Full Spectrum Survivability and Lethality Baseline Test Reporting Requirements, Continued

Topic	Information
Recoverability	• Report on the effectiveness and timeliness of the user or DoD system response action to the attack. Detail the effectiveness of the actions to recover the DoD system, the time it takes to recover the DoD system, and the residual operational effectiveness and suitability post recovery. List if recovery operations provide full or decremented capability. Quantify metrics and measures as appropriate and include: – Organization or users performing response action. – Activity prompting response (e.g., detection, white card, false alarm). – Reaction (e.g., incident report, block access, remove system). – Outcome of response action (e.g., adversary access removed, malware removed, response action failed, equipment repaired, mission restored). Include the evaluation of any backup systems and if the backup systems were affected by the attack. – Appropriateness of the recovery action. – Response timelines – initiation to completion. – Any negative impacts on operations from defensive actions themselves. – Any white cards used for collecting response data and results of those actions upon mission performance. – TTP to counter the attack, as applicable. – Measured or observed data on maintenance and update processes expected during sustainment to maintain survivability. – Measured or observed data on actual (or anticipated) actions demonstrating the ability to adapt and prevent the recurrence of attacks, as applicable. • For cyberspace attacks or EMS attacks, list any modifications to the DoD system that would thwart the reintroduction or repeat of a cyberspace or EMS attack. • For EMS, evaluate the EMS integrated reprogramming process and its ability to update and distribute new identification information (e.g., EMS signatures) to platforms and systems.
Lethality	• Report on the assessment of the adversaries' ability to degrade the lethal effects due to, among other things, their situational awareness, signature management, or defensive capabilities on the DoD systems' offensive lethal effects. • Report on the ability of the offensive capability to deny, degrade, disrupt, deceive, destroy, exploit, or influence each of the operationally relevant target categories including the lethal effects on the target's firepower, mobility, communications, and other mission critical functions, as applicable. Include the type and the number of weapons on the target required to degrade or destroy target's firepower, mobility, communications, and other mission critical functions, as applicable. • Report on any changes to the lethal effect as fired from the platform or by the user. • Report on the effect of the lethal effects on collateral damage. • Report the EP techniques employed by the adversary system and the EA techniques they were designed to counter. • For EA techniques, report the effects observed before and after the EP technique was implemented. • For EA techniques, report the threshold (e.g., jam-to-signal ratio) and the length of time required for the EA technique to produce a desired effect on the receiver given the EP techniques implemented by the receiver.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AI	artificial intelligence
CBRN	chemical, biological, radiological, and nuclear
CT&E	contractor test and evaluation
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DOT&E	Director of Operational Test and Evaluation
DT&E	developmental test and evaluation
E3	electromagnetic environmental effects
EA	electromagnetic attack
EM	electromagnetic
EMS	electromagnetic spectrum
EP	electromagnetic protection
FUSL	full-up system-level
GPS	global positioning system
IDSK	integrated decision support key
ITT	integrated test team
LFT&E	live fire test and evaluation
M&S	modeling and simulation
MBRA	mission-based risk assessment
MIL-STD	military standard
NATO	North Atlantic Treaty Organization
OT&E	operational test and evaluation
OTA	operational test agency
T&E	test and evaluation
TEMP	test and evaluation master plan
TTP	tactics, techniques, and procedures

ACRONYM	MEANING
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering
V&V	verification and validation
WG	working group
WIPT	working-level integrated product team

G.2. DEFINITIONS.

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

TERM	DEFINITION
abbreviated injury scale	An anatomical-based coding system created by the Association for the Advancement of Automotive Medicine to classify and describe the severity of injuries. It represents the threat to life associated with the injury rather than the comprehensive assessment of the severity of the injury.
accreditation	Defined in DoDI 5000.98.
acquisition decision	Defined in DoDI 5000.98.
adversarial test	Identifies new vulnerabilities or exploits predicted vulnerabilities during the mission execution in the presence of opposing forces and capabilities emulating the adversary. Evaluates the performance of self-defense systems, trained operators including defenders, and the ability of the unit equipped with the system to identify and respond to the adversary.
congested environment	Defined in DoDI 5000.98.
constrained environment	Defined in DoDI 5000.98.
contested environment	Defined in DoDI 5000.98.

TERM	DEFINITION
cooperative test	Identifies new or exploits predicted vulnerabilities and their effect on operational effectiveness, suitability, survivability, and lethality (if applicable) in an overt manner using live kinetic or non-kinetic threats. Conducted at the sub-component, component, sub-system, system level using prototypes or early system configurations, and FUSL. Takes into consideration susceptibility to attack, the performance of self-defense systems, and evaluates the performance of defenders and recoverability teams or capabilities. Evaluates user casualties, as applicable.
cyberspace	A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
cyberspace attack	Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain and is considered a form of fires.
cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation.
cybersecurity service provider	An organization that provides one or more cybersecurity services to implement and protect the DoD information network.
derived requirements	These requirements arise from constraints; consideration of issues implied but not explicitly stated in the requirements baseline; factors introduced by the selected architecture; cybersecurity requirements; and design. Derived requirements are definitized through requirements analysis as part of the overall DoD systems engineering process and are part of the allocated baseline.

TERM	DEFINITION
E3	The impact of the EM environment upon the operational capability of military forces, equipment, DoD systems, and platforms. E3 addresses effects from EM compatibility, EM interference, EM vulnerability, EM pulse, EP, electrostatic discharge, and hazards to personnel, ordnance, and fuels or volatile materials. E3 includes the effects generated by all EMS operational environment contributors including radio-frequency systems, ultra-wideband devices, high-power microwave systems, lightning, and precipitation static.
EM attack	Division of EM warfare involving the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.
EM compatibility	The ability of DoD systems, equipment, and devices that use the EMS to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of EM radiation or response.
EM interference	Any EM disturbance induced intentionally or unintentionally that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment.
EMS	A maneuver space essential for facilitating control within the operational environment that impacts all portions of the operational environment and military operations. The range of frequencies of EM radiation covers is from zero to infinity. Unique naming conventions exist for the various band designations within the EMS with each being established due to a variety of historical, physical, or practical purposes. In practical terms, EMS refers to the totality of all possible radiant EM energy.
EMS-dependent system	All electronic systems, sub-systems, devices, or equipment that depend on the use of the spectrum to properly accomplish their function(s) without regard to how they were acquired (e.g., full acquisition, rapid acquisition, joint concept technology demonstration) or procured (e.g., commercial off-the-shelf, government off-the-shelf, non-developmental items).

TERM	DEFINITION
EMS management	The operational, engineering, and administrative procedures to plan and coordinate operations within the EM operational environment.
EM support	Division of EM warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.
EP	Division of EM warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.
FUSL test	Defined in DoDI 5000.98.
IDSK	Defined in DoDI 5000.98.
integrated T&E	Defined in DoDI 5000.98.
kill chain	Defined in DoDI 5000.98.
kinetic threat	Defined in DoDI 5000.98.
laser clearinghouse	United States Air Force Strategic Command organization that provides predictive avoidance analysis and deconfliction with U.S. and allies satellites and operations.
LFT&E	Defined in DoDI 5000.98.
live data	Defined in DoDI 5000.98.
maintainability demonstration	A formal process conducted by the product developer and the end customer to determine whether specific maintainability requirements in the system specifications have been achieved. Demonstration testing requires a formal test plan be developed that uses defined methods of analysis to determine compliance.
model	Defined in DoDI 5000.98.

TERM	DEFINITION
M&S verification, validation, and accreditation	Defined as "M&S VV&A" in DoDI 5000.98.
multi-domain operations	Defined in DoDI 5000.98.
national vulnerability database	The U.S. Government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol. This data enables automation of vulnerability management, security measurement, and compliance. It includes databases of security checklist references, security-related software flaws, product names, and impact metrics.
non-kinetic threat	Defined in DoDI 5000.98.
operational effectiveness	Defined in DoDI 5000.98.
operational suitability	Defined in DoDI 5000.98.
operationally relevant	Defined in DoDI 5000.98.
operationally representative	Defined in DoDI 5000.98.
OT&E	Defined in DoDI 5000.98.
penetration testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a DoD system.
program decisions	Defined in DoDI 5000.98.
program manager	Defined in DoDI 5000.98.
realistic full spectrum lethality	Defined in DoDI 5000.98.
realistic full spectrum survivability	Defined in DoDI 5000.98.
recoverability	Defined in DoDI 5000.98.

TERM	DEFINITION
Red Team Action Map	The working report for certified Cyber Red Team activities during all operations, including during the reconnaissance phase. Action Map nodes and links include data elements describing the Cyber Red Team activities, position, and access.
risk-based level of testing	Defined in DoDI 5000.98.
scientific rigor	Defined in DoDI 5000.98.
simulation	Defined in DoDI 5000.98.
supply chain	A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
supply chain risk	The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system.
susceptibility	Defined in DoDI 5000.98.
system-of-systems	Defined in DoDI 5000.98.
T&E Oversight List	Defined in DoDI 5000.98.
T&E resources	Defined in DoDI 5000.98.
TTP	Patterns of behavior used to create a standard way of operating. TTP can also be adversarial patterns used to gain actionable intelligence against an enemy style of attacking.
validation	Defined in DoDI 5000.98.
verification	Defined in DoDI 5000.98.
vulnerability	Defined in DoDI 5000.98.

TERM	DEFINITION
white card	Simulated event in a test. White cards are used when pursuing an exploitation or penetration of DoD system(s) where live testing is expensive and impractical.

REFERENCES

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020, as amended

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

DoD Directive 5205.07 "Special Access Program (SAP) Policy," July 1, 2010, as amended

DoD Instruction O-3600.03, "Test and Evaluation of Cyberspace Effects and Enabling Capabilities," January 19, 2022

DoD Instruction 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum," January 9, 2009, as amended

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, as amended

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

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

DoD Instruction 8585.01, "DoD Cyber Red Teams," January 11, 2024

DoD Manual 5000.102, "Modeling and Simulation Verification, Validation and Accreditation in Test and Evaluation," December 9, 2024

DoD Manual 5000.100, "Test and Evaluation Master Plans and Test and Evaluation Strategies," December 9, 2024

DoD Responsible AI Working Council, "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway," June 2022

Joint Publication 3-85, "Joint Electromagnetic Spectrum Operations," May 22, 2020

Military Handbook MIL-HDBK-235-8, "Military Operational Electromagnetic Environment Profiles," April 3, 2018

Military Standard MIL-STD-461G, "Interference Characteristics Requirements for Equipment," December 11, 2015

Military Standard MIL-STD-464D, "Electromagnetic Environmental Effects Requirements for Systems," December 24, 2020

Military Standard MIL-STD-1553C, "Digital Time Division Command/Response Multiplex Data Bus," February 28, 2018

Military Standard MIL-STD-2169D, "High-Altitude Electromagnetic Pulse (HEMP) Environment," March 31, 2020

Public Law 117-81, Section 223, "National Defense Authorization Act for Fiscal Year 2022," December 27, 2021

Public Law 116-283, Section 1712, "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 1, 2021

Secretary of Defense Memorandum, "Artificial Intelligence Ethical Principles for the Department of Defense," February 21, 2020

United States Code, Title 10