DoW Manual 5000.103

Cyber Developmental Test and Evaluation

Originating Component:	Office of the Under Secretary of War for Research and Engineering
Effective:	February 25, 2026
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved 02/19/2026 by:	Emil Michael, Under Secretary of War for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02 and DoD Instruction (DoDI) 5000.89, this issuance implements policy, assigns responsibilities, and prescribes procedures for cyber developmental test and evaluation (DT&E).

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSW, 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 DoW Field Activities, and all other organizational entities within the DoW (referred to collectively in this issuance as the "DoW Components").

1.2. POLICY.

DoDIs 5000.89 and 8500.01 establish the requirement to conduct cybersecurity DT&E of DoW systems to support assessments of cybersecurity, survivability, and resilience within a mission context. In accordance with DoDI 5000.89, this issuance prescribes the procedures and processes for DoW Components to plan, fund, execute, and report on cyber DT&E.

SECTION 2: RESPONSIBILITIES

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

Pursuant to Section 133a of Title 10, United States Code (U.S.C.), and in accordance with DoDD 5137.02 and DoDI 5000.89, the USW(R&E):

a. Reviews and approves exceptions and procedural deviations from this issuance for all systems, projects, and services (referred to in this issuance as "systems") on the Test and Evaluation (T&E) Oversight List for DT&E available at https://www.dote.osd.mil/Oversight/, for which the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) is the milestone decision authority.

b. Approves the cyber DT&E plan in the T&E master plan (TEMP) or the T&E strategy for all acquisition category ID programs.

c. Advises the decision authority on the cyber DT&E plan's sufficiency in the TEMP or T&E strategy for non-acquisition category ID programs on the T&E Oversight List for DT&E.

d. Serves as the Principal Staff Assistant for the cyber test ranges, overseeing the Director for the Test Resource Management Center as the DoD Executive Agent for Cyber Test Ranges, in accordance with DoDD 5101.19E.

e. Coordinates with the USW(A&S), the Under Secretary of War for Intelligence and Security (USW(I&S)), the Director of Operational Test and Evaluation, the DoW Chief Information Officer (DoW CIO), and the Chief Digital and Artificial Intelligence Officer (CDAO) to synchronize the processes in this issuance with the:

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

(2) DoD Strategic Cybersecurity Program in accordance with Section 1640 of Public Law (PL) 115-91.

(3) DoD Data, Analytics, and Artificial Intelligence (AI) Adoption Strategy and the DoD Responsible AI Toolkit.

(4) DoW intelligence processes in support of science and technology (S&T) and the Defense Acquisition System.

(5) Other Defense Acquisition System processes and throughout the defense industrial base.

2.2. CDAO.

Under the authority, direction, and control of the USW(R&E), the CDAO coordinates with the USW(A&S), the USW(I&S), and the DoW CIO to synchronize the processes in this issuance with the DoD Data, Analytics, and AI Adoption Strategy and the DoD Responsible AI Toolkit.

2.3. USW(A&S).

The USW(A&S):

a. Coordinates with the USW(R&E), the DoW CIO, the USW(I&S), and the CDAO to implement and synchronize requirements of this issuance as specified in Paragraph 2.1.e.

b. Develops, institutes, and enforces contracting language policy and guidance supporting cyber DT&E.

2.4. USW(I&S).

The USW(I&S):

a. Coordinates with the USW(R&E), the USW(A&S), the DoW CIO, and the CDAO to synchronize the processes in this issuance as specified in Paragraph 2.1.e.

b. Develops, institutes, and enforces cyberspace threat intelligence support for cyber DT&E.

2.5. DIRECTOR OF OPERATIONAL TEST AND EVALUATION.

Pursuant to Sections 139, 4171, and 4172 of Title 10, U.S.C., the Director of Operational Test and Evaluation coordinates cyber T&E policy, guidance, and procedures with the USW(R&E).

2.6. DOW CIO.

The DoW CIO:

a. Coordinates with the USW(R&E), the USW(A&S), the USW(I&S), and the CDAO to synchronize the processes in this issuance as specified in Paragraph 2.1.e.

b. Develops, institutes, and enforces cybersecurity policy and guidance supporting cyber DT&E.

2.7. DOW COMPONENT HEADS.

The DoW Component heads:

a. Oversee Component chief information officers, program managers, project managers, S&T managers or equivalent, contracting officials, system security practitioners, chief developmental testers (CDTs) or other T&E leads, and designated DT&E organization leads implementing this issuance in accordance with DoDI 5000.89 throughout system development.

b. Ensure Component acquisition executives and chief information officers enforce the procedures for cyber DT&E of DoW systems in accordance with this issuance, complement the Component procedures for implementing the DoD Cybersecurity Program in accordance with DoDI 8500.01, the DoD Risk Management Framework (RMF) in accordance with DoDI 8510.01, and complement procedures for mission assurance in accordance with DoDI 3020.45.

c. Ensure Component program managers, project managers, S&T managers, or equivalent integrate cyber test planning and cyber test execution across stakeholders to facilitate efficient data and resources usage, in accordance with DoDI 5000.89.

d. For systems and acquisition programs not on the T&E Oversight List for DT&E, determine the authorities responsible for approval of cyber DT&E plans in the TEMP or T&E strategy.

e. Prescribe DoW Component-specifics for:

(1) Technical proficiency, training standards, requirements, and required certification for personnel performing cyber DT&E in accordance with DoDD 8140.01, DoDI 8140.02, and DoDI 8585.01.

(2) The processes and data requirements for verifying and validating modeling and simulation (M&S) to support accreditation in accordance with DoDI 5000.61.

(3) When and to whom program managers, project managers, S&T managers, or equivalent will deliver cyber DT&E plans and reports.

f. Require cyber DT&E before all DoD RMF authorization decisions throughout a system's life cycle.

g. Ensure cyber DT&E planning and data informs:

(1) Realistic full spectrum survivability evaluations of covered systems in accordance with Section 4172 of Title 10, U.S.C., and Section 223 of PL 117-81.

(2) Operational effectiveness and suitability evaluations.

SECTION 3: CYBER DT&E OVERVIEW

3.1. GENERAL.

This issuance emphasizes initiating testing early and iteratively throughout the system's lifecycle and ensuring mission-focused cyber DT&E. Cyber DT&E:

a. Applies to all DoW systems, including:

(1) Non-acquisition and pre-acquisition program technology, system, and capability development starting in mission engineering, S&T, prototyping and experimentation, and any development for eventual insertion into DoW networks, systems, platforms of systems, and system-of-systems.

(2) Acquisition systems in accordance with the DoDD 5205.07.

(3) Systems acquired via the Defense Acquisition System, including abbreviated acquisition programs under the U.S. Navy or U.S. Marine Corps and acquisitions pursuing any adaptive acquisition framework pathway in accordance with DoDD 5000.01 and DoDI 5000.02.

(4) Systems in sustainment, or post productions systems, when those systems have changes as outlined in Paragraph 3.2.a.(13).

b. Supports:

(1) Providing program engineers and decision-makers with information to measure system developmental progress, identify problems, characterize system capabilities and limitations, and manage technical and programmatic risks.

(2) Designing and executing iterative system developer (contractor) and government cyber DT&E, including M&S, and life cycle re-assessment events, as appropriate.

(3) Iterative and recursive evaluation of a system's cybersecurity and cyber resilience performance requirements in support of assigned missions. Cyber DT&E activities support data generation for independent evaluation of the requirements for a system's ability to:

(a) Prevent cyberspace events from causing the degradation or failure of mission or safety critical functions or operational mission impacts.

(b) Detect anomalies caused by cyberspace events.

(c) Determine the cause of the anomaly, system misconfigurations, or design flaws.

(d) Report sufficient facts about the cyberspace event to mitigate the anomaly or design flaw to a responsible entity, which may be a non-person entity.

(e) Enable the responsible entity to mitigate a reported anomaly during and after an operational mission.

(f) Recover from the degradation or loss of mission or safety critical functions and maintain operational resilience in cyberspace throughout a system's life cycle.

(4) Using cyber DT&E data to perform quantitative analysis of system performance degradations.

c. Events iteratively employ a variety of cooperative and adversarial tactics and techniques. Use of adversarial tactics in test events will be collaborative to ensure optimal use of limited testing periods.

d. Event results will provide timely knowledge to inform decisions which may include:

(1) Capability development and transition decisions for pre-acquisition program technologies and systems.

(2) Design trades.

(3) Acquisition decisions (e.g., production, manufacturing, operation, or sustainment).

(4) Risk acceptance and authorizations decisions.

(5) Integration of systems into platforms.

(6) An evaluation of a system's ability to meet its technical performance requirements despite cyberspace events.

(7) The evaluation of realistic full spectrum survivability and lethality (FSSL) in contested cyberspace for covered systems in accordance with Section 4172 of Title 10, U.S.C., and Section 223 of PL 117-81.

(8) Future cyber test requirements and updates to T&E strategies based on mission needs, changing threat, operational conditions, etc., as discussed in Paragraph 3.2.a.(13).

e. Planning is the responsibility of the T&E working-level integrated product team (WIPT), or integrated test team (ITT) as appropriate, supported by a cyber working group (CyWG) leading the overall cyber T&E process.

f. Does not replace the requirement to perform realistic FSSL T&E and operational T&E (OT&E).

3.2. CYBER DT&E.

a. Overview.

Plan cyber DT&E events, as applicable, using a test-fix-test approach across the system life cycle to:

(1) Include cyber DT&E conducted by both the system developer (contractor) and government and integrated contractor/government T&E when appropriate.

(2) Ensure test teams independent of the system development perform the testing and are qualified pursuant to DoDD 8140.01 and DoDI 8585.01, as required.

(3) Use data from the system developer (contractor) and the program, project, S&T, or equivalent security verification and continuous monitoring efforts in accordance with DoDI 5000.79. Security verification includes:

(a) Security technical implementation guide scanning.

(b) Software assurance processes in accordance with DoDI 5000.83. Automated software assurance scripts used for software developed under agile processes with continuous integration will inform individual cyber DT&E plans.

(c) Other methods to identify known vulnerabilities and exposures in the system including, but not limited to, code analysis tools and techniques (automated or not) and tracking cyber deficiencies over time.

(4) Assess CyWG prioritized subcomponents, components, subsystems, systems, and system-of-systems iteratively and recursively, as applicable, with a mission-context, informed by mission-based cyber risk assessments (MBCRAs) in accordance with DoDI 5000.89, to identify exploitable cyberspace vulnerabilities and other system faults in the system under test.

(5) Measure and verify specified performance requirements in representative contested cyber environments, including disrupted, disconnected, intermittent, and low bandwidth, and include realistic data and communication flows where the responsible cyber DT&E team employs representative cyberspace threat tactics, techniques, and procedures (TTPs) against the system under test's defensive capabilities with the intent to cause mission effects.

(6) Measure and verify specified cyber performance requirements for system capabilities to prevent, detect, contain, mitigate or eliminate, and recover from the loss of mission or safety critical functions in required mission timelines, in accordance with DoDI 8530.03.

(7) Evaluate the effects of cyberspace attacks and other system faults which may lead to cascading effects (including collateral effects) in both the physical and cyberspace domains.

(8) Inform program managers and capability stakeholders about the technical risks of vulnerabilities and identified system faults affecting mission execution, system availability, recoverability, and overall cyber resilience.

(9) Identify engineering and technical cyber risks in the system and attack surface components.

(10) Use cooperative and adversarial tactics informed by available current threat intelligence and prior cyber test results. When conducting both cooperative and adversarial cyber DT&E in a planned test, often called "purple team testing," deconflict cooperative activities from adversarial activities to minimize potential negative impacts to testing.

(11) Evaluate attempts to circumvent or defeat the system's security features under specific conditions defined by the system or mission owner and the testers.

(12) Verify products are compliant with security technical implementation guides and analyze exposures to known vulnerabilities within the National Vulnerability Database in accordance with DoDI 8531.01.

(13) Assess changes to cybersecurity and cyber resilience risks resulting from:

(a) Recurring software releases.

(b) System and architecture modifications.

(c) System baseline upgrades.

(d) Evolving or emerging threat capabilities.

(e) Newly identified vulnerabilities.

(f) New cyberspace attack vectors.

(g) New cyberspace attack TTPs.

(h) New components or changes to components within the authorization boundary.

(i) Changes to existing technology, or introduction of new technology, and technology enhancements, including life cycle replacement of hardware no longer on the approved products list.

(j) External interfacing systems including vendor and government supply chains, system's development environment, software factories, interconnection agreements, and all software distribution channels and processes.

(k) Changes to the operational mission performance requirements, concept of operations, concept of employment, or other operational mission information (e.g., mission essential task lists), as applicable.

(14) Verify vulnerability remediation and mitigation efforts in accordance with DoDI 8531.01 and ensure fixes do not introduce exploitable weaknesses.

(15) Assess effects of simultaneous exploitation of multiple vulnerabilities, weaknesses, system faults, and attack paths across system components, or across multiple systems on a platform.

(16) Use representative operators, maintainers, and defenders, as applicable or practicable, to assess system and proxy defenders' ability to prevent, detect, contain, mitigate or eliminate, and recover the loss of mission or safety critical functions.

(17) Inform every DoD RMF authorization decision.

b. Government Acceptance Cyber T&E.

Government acceptance cyber T&E (which may include both government DT&E and government OT&E) will:

(1) Verify and evaluate the specified requirements for system capabilities to prevent, detect, contain, mitigate or eliminate, and recover from the loss of mission or safety critical functions in required mission timelines for the delivered system under test (e.g., minimum viable capability release, subsequent software release, increment, or another intermediate deliverable) before proceeding into government DT&E.

(2) Include system developer (contractor) and government technical, operational, system development, test environment, threat representative, and threat intelligence personnel, and the appropriate supply chain risk management office.

(3) Validate the implementation of any technical security controls in scope and cyber performance requirements.

(4) Employ a digital twin of the system, a system integration lab or hardware in-the-loop facility, or other test asset to sustain cyber DT&E throughout a system's life cycle.

(5) Inform the decision to accept the product.

c. Government Cyber DT&E.

The government cyber DT&E program will be in accordance with DoDI 5000.89 and will:

(1) Include a multi-disciplinary team of system T&E specialists, technical personnel, and other required personnel, including specialists related to unique technologies in the system under test and data collectors, from the system developer (contractor) and the government.

(2) Measure and evaluate the technical requirements to prevent, detect, contain, mitigate or eliminate, and recover from the loss of mission or safety critical functionality for components, subsystems, prototypes, and developmental systems continuing to mature and undergo design changes.

(3) Use network architecture documentation, functional data flows, and digital engineering models from interfacing systems to support verifying the system meets its mission and functional performance specifications.

(4) Evaluate the draft technical procedures for installing software, firmware, or hardware updates, and procedures for verifying system configurations to inform any required modifications to the procedures.

(5) Evaluate system cyber defender procedures, available system training materials, and planned defensive tools.

(6) Use known and newly discovered vulnerabilities and exposures, based on current threat intelligence, the National Vulnerability Database, and available information on known exploits, to attempt impacts on mission or safety critical components, subsystems, and the developmental system.

(7) When possible, provide responsible cyber DT&E teams direct access to the tactical systems (e.g., tactical vehicles, aircraft) under test configured as operationally realistic as possible.

(8) Early in developmental testing and for enterprise and cloud networks, use cyber ranges, M&S, system developer (contractor) test labs, and DoW Component test facilities to better understand impacts of cyberspace threats to mission operations. Cyber ranges, system integration labs, and hardware-in-the-loop facilities provide cost effective environments, while minimizing risk to operational assets.

(9) Use digital system engineering models, appropriate tools, and regression testing to evaluate the effectiveness of fixes (e.g., remedies or mitigations implemented to eliminate or reduce the risk presented by previously identified vulnerabilities and other deficiencies).

(10) Finish verifying fixes and cyber performance requirements before the final operational test readiness review.

(11) Use data and results of government cyber DT&E, as applicable, to inform development related decisions, DoD RMF security control assessments, risk and authorization decisions, realistic FSSL T&E and OT&E planning, and deployment or fielding decisions.

d. Integrating Cyber Testing.

(1) Integrating or combining cyber testing requires the collaborative planning, preparation, and execution of test events to provide shared data in support of independent analyses, evaluation, and reporting by all stakeholders.

(2) To the maximum extent possible, plan and execute cyber DT&E to leverage integrated testing.

(3) Integrated cyber tests can include:

(a) Integrated system developer (contractor) and government cyber developmental test. At a minimum, the government will observe all system developer (contractor) cyber DT&E.

(b) Integrated government cyber testing where the DT&E and OT&E organization(s) independently evaluate the data.

(c) Combined cyber testing using threat representative tactics and techniques concurrently with other testing including functional performance, interoperability, and other non-functional operational and support requirements (e.g., reliability, availability, maintainability, supportability).

3.3. INTEGRATION WITH DOD RMF.

a. The DoD RMF process supports gaining and retaining an interim authorization to test (IATT), authorization to connect, authority to operate (ATO), or processes for the DoD RMF "Assess Only" in accordance with DoDI 8510.01.

b. DoD RMF processes will not replace or supersede the procedures in this issuance. Cyber DT&E procedures, data, and artifacts will inform DoD RMF and compliance efforts.

c. The DoW cyber DT&E and DoD RMF processes and artifacts will complement each other as part of the DoD Cybersecurity Program.

d. Cyber DT&E conducted using closed loop test ranges is equivalent in all respects to testing in a pre-production or developmental test environment and does not require an IATT, ATO, any other cybersecurity certification attestation, or the use of a certified and accredited DoW cyber red team, in accordance with DoDI 8585.01.

e. In accordance with DoDI 8510.01, the technology or system will complete the RMF assessment procedures for the DoD RMF "Assess Only," IATT, authorization to connect, ATO with conditions, or ATO, as required, to connect and operate a system before the final operational test readiness review.

f. Program managers, project leads, S&T managers, or equivalent will provide the authorizing official all current cyber DT&E results to support every ATO decision.

3.4. CYBER DT&E AND M&S.

a. M&S may be a component of cyber DT&E. When M&S is used as part of cyber DT&E, the T&E WIPT or ITT as appropriate, in coordination with the accreditation authorities, will integrate M&S capabilities, including cyber test ranges, digital twins, or models with system developer (contractor) cyber T&E and government cyber DT&E. When feasible, M&S will support the evaluation of:

(1) System weaknesses and vulnerabilities.

(2) Access to the system weaknesses, including access from interoperable, integrated, or connected systems and system-of-systems.

(3) Emulation of adversary capabilities to assess cyberspace threat emulated effects on interoperable, integrated, or connected systems, systems-of-systems, families of systems, and platforms of systems, and the ability for systems to support mission completion.

b. When M&S is used as part of cyber DT&E, the TEMP or T&E strategy will describe the M&S verification, validation, and accreditation requirements and relevant M&S verification and validation plans, in accordance with DoDIs 5000.61 and 5000.89.

c. M&S teams will use data from cyber tests of actual system(s) under test (e.g., during government DT&E, OT&E, or realistic FSSL T&E) to verify M&S identified and non-remediated deficiencies.

3.5. CYBER DT&E PROGRAM MANAGEMENT.

a. Program Manager, Project Lead, S&T Manager, or Equivalent.

The program manager, project lead, S&T manager, or equivalent will:

(1) Follow the DT&E procedures in accordance with DoDI 5000.89 and this issuance.

(2) Identify the cybersecurity lead and charter a CyWG at the initiation of S&T research, pre-acquisition projects, acquisition programs, or before any contractual commitment or release of the first request for proposal (RFP), to support the T&E WIPT, or ITT as appropriate, in planning and executing cyber T&E (which includes any instance of, or combination of, contractor or government cyber DT&E and cyber OT&E).

(3) Require the CyWG to plan and monitor cyber DT&E as described in this issuance, including DT&E for complex platforms integrating multiple systems into a platform with interoperable enclaves or authorization boundaries (e.g., U.S. Navy ships, fighting vehicles, cyberspace operations platforms, and cloud platforms as a service).

(4) Confirm integration of the DoD RMF and cyber T&E processes to support the DoD Cybersecurity Program.

(5) Consider including supporting cyber test agencies as members of the systems security working group (or equivalent) if formed to support system security engineering.

(6) Ensure contract(s) and other transactions include cyber DT&E requirements including, but not limited to, items in Paragraph 4.2.b.

(7) Decide actions based on the government acceptance cyber T&E recommendations regarding products with vulnerabilities needing remediation or mitigation.

(8) Provide resources and confirm schedules across the life cycle to enable government organizations to support all efforts in Section 4 for cyber DT&E iterative planning, preparation, execution, remediation of findings, and retesting.

(9) Plan to use existing government tools or fund required cyber T&E tool development, procurement, and authorization to support planned government cyber T&E.

(10) Plan for, fund, and maintain required operationally representative cyber test infrastructure and environments (e.g., cloud developmental test environments, system integration lab or hardware in-the-loop facility, or digital twins) throughout a system's life cycle.

(11) Coordinate with the DoD Executive Agent for Cyber Test Ranges, in accordance with the DoDD 5101.19E, to plan, schedule, and employ range infrastructure, as appropriate.

(12) Plan and resource for disposable or restorable test articles as needed to support destructive cyber testing of mission or safety critical assets.

(13) Coordinate and confirm operationally representative data flows for integrated or interfacing systems are available for the cyber DT&E events, whether as part of the system under test or as systems supporting the test.

(14) Obtain an IATT, obtain an ATO, or complete the RMF assessment procedures for the DoD RMF "Assess Only" if required to perform government cyber DT&E.

(15) Integrate testing results into cybersecurity processes during development. Provide all cyber T&E results to decision authorities and authorizing officials.

(16) Track all cyber deficiencies in the Joint Deficiency Reporting System or other DoW Component deficiency reporting database (e.g., enterprise mission assurance support service), at the correct classification level in accordance with the appropriate security classification guide. Report and track findings not adjudicated as deficiencies in enterprise mission assurance support service or equivalent databases to support the DoD RMF process.

(17) Employ real or simulated operational interfaces, when applicable, during cyber DT&E to inform joint interoperability certification in accordance with DoDI 8330.01.

(18) Maintain and make available to authorized users all documentation, artifacts, T&E data, and system developer (contractor) delivered data. Manage all cyber T&E data and documentation in accordance with DoDI 5015.02.

(19) Provide access to all cyber T&E reports to decision authorities, oversight authorities, operational test agencies or organizations, and appropriate authorizing officials for consideration during risk acceptance and authorizations decisions in accordance with DoDI 8510.01.

b. CyWG.

The CyWG, or an equivalent entity under a different name, will support the T&E WIPT or ITT responsibilities defined in DoDI 5000.89. The CyWG will:

(1) Provide cyber DT&E data, risk assessments, deficiencies, and all test results to the program manager, project manager, S&T manager, or equivalent to inform decisions.

(2) Plan to maximize integrated government developmental, live fire, and operational cyber T&E.

(3) Include specialized cyber expertise to support the T&E WIPT or ITT with planning, execution, and analysis of cyber DT&E.

(4) Include experts, as appropriate, in non-enterprise systems (e.g., embedded, real-time operating systems, non-Internet Protocol (IP) systems, AI technologies, cloud technologies, control systems, cyber physical systems, critical infrastructure, operational technology, communications including tactical communications, other bus-based systems, and supply chain risk management).

(5) Support working groups (e.g., system security) or integrated product teams with cyber T&E representation, as appropriate.

(6) Perform planning activities detailed in Paragraph 4.2., verify cyber DT&E preparation, and coordinate with the program manager, project manager, S&T manager or equivalent, or T&E lead regarding cyber DT&E funding, planning, scheduling, execution, analysis, evaluation, and reporting in support of overall T&E and engineering planning.

(7) Support efforts to conduct criticality, vulnerability, and supply chain analyses in accordance with DoDIs 5000.83 and 5200.44. Ensure such analyses identify mission-relevant terrain in cyberspace (MRT-C) in accordance with DoDI 3020.45 and includes subcomponent investigation and supply chain document reviews.

(8) Characterize the attack surface using all available system architectures and artifacts to identify all forms of communication, network connectivity, software, hardware, supply chain, and human interaction.

(9) Confirm cyber T&E informs the S&T approach or acquisition strategy, cybersecurity strategy, engineering plans, and other plans.

(10) Define cyber DT&E requirements and resources (e.g., support to MBCRA, system developer (contractor) cyber DT&E, government cyber DT&E, digital representations, test articles, schedule, infrastructure, data) for inclusion in RFPs, contracts, and other agreements.

(11) Review and provide assessments on system developer (contractor) cyber test plans to the T&E WIPT or ITT.

(12) Observe and track progress of system developer (contractor) cyber T&E to ensure consistency with the TEMP or T&E strategy.

(13) Identify and coordinate with the lead DT&E organization to ensure availability of required government cyber T&E tools to support planned government cyber DT&E.

(14) Review relevant documentation (e.g., system concept of operations, networks, interfaces, architectures, program protection plans (PPPs), software and hardware assurance test results, supply chain processes, bills of materials (BOMs), and supply chain systems for the system under test) starting at the initiation of the project or acquisition program and recurringly throughout the system's life cycle.

(15) Request support from, and collaborate with, the appropriate intelligence resource to conduct system threat analyses.

(16) Use MBCRAs to conduct an attack path analysis and develop a cyber DT&E prioritization for testing critical subcomponents and data through systems-of-systems, using:

(a) The attack surface characterization.

(b) The criticality analysis and identified mission or safety critical functions, including the identified MRT-C.

(c) The system threat assessment and the validated online life cycle threat report, as available.

(d) All available system design information.

(e) Existing and known vulnerabilities.

(17) Ensure MBCRA results inform the next developmental or engineering decision and future cyber T&E.

(18) Provide cyber DT&E input to TEMP or T&E strategy development, including the plan for MBCRAs and the cyber DT&E equities in the integrated decision support key (IDSK).

(19) Identify which critical systems, subsystems, or components will undergo cyber DT&E throughout the system's life cycle, as the system and the cyberspace threats evolve. For systems developed and implemented as part of larger platforms of systems, the system program offices will maintain current versions of all system documentation throughout the platform development to support cyber T&E planning with the platform owner.

(20) Provide recommendations to the program manager, project manager, S&T manager, or equivalent for all identified system deficiencies that compromise operational resilience in cyberspace.

c. CDT or T&E Lead.

The CDT or T&E lead:

(1) Designates the responsible cyber DT&E team.

(2) As an integral part of overall development activities, coordinates the planning, management, and oversight of all cyber DT&E activities.

(3) Approves government cyber DT&E plans. For integrated government cyber T&E events, ensures responsible test team(s) develop separate objectives for DT&E, realistic FSSL T&E, and OT&E, as applicable, for approval by the appropriate authorities.

d. Responsible Cyber DT&E Team.

The responsible cyber DT&E team will:

(1) Provide technical expertise on cyber DT&E concerns to the CDT or T&E lead.

(2) Collaborate with the system developer as appropriate, coordinate across facilities, organizations, and personnel supporting government cyber DT&E events, and support all cyber DT&E activities as a member of the CyWG.

(3) Train and provide qualified cyber DT&E personnel in coded positions, in accordance with DoDD 8140.01, DoDI 8140.02, and DoDI 8585.01, as required.

(4) Support the CyWG and the activities in Paragraph 4.2.

(5) Plan cyber DT&E to verify MBCRA results in addition to completing other cyber DT&E objectives and identifying additional vulnerabilities within the test scope.

(6) Develop the government cyber DT&E plans.

(7) Conduct government cyber DT&E preparation.

(8) Perform government DT&E cyber test execution, analysis, evaluation, and reporting.

(9) Support DoD RMF assessment and authorization activities.

(10) Help the CDT or T&E lead:

(a) Oversee system developer (contractor) cyber DT&E.

(b) Reach technically informed, objective judgments about system developer (contractor) and government cyber DT&E planning and results.

(11) Inform and support the security verification approach to ensure continuous monitoring data informs system developer (contractor) cyber T&E and government cyber DT&E.

(12) As part of government acceptance cyber T&E, provide a recommendation to the program manager, project manager, S&T manager, or equivalent whether to accept products with vulnerabilities posing a risk to the mission or to safety critical functions or to return the product to the system developer (contractor) for remediation or mitigation. Other vulnerabilities may also lead to recommendations of non-acceptance, based on the level of risk determined by the test team's evaluation of test data.

(13) Baseline system performance before cyber tests. Baselining may include compromise hunting, through which experts examine the system, components, software, etc. for malicious code, backdoors, or evidence of prior or existing intrusions before cyber testing.

(14) Identify indicators of compromise or attempted exploitation while validating threat TTPs to enable operators and defenders to mitigate known vulnerabilities or weakness when remediation of identified vulnerabilities or weaknesses is not possible.

(15) Analyze test plan deviations for impacts on evaluating the system's cybersecurity and resilience performance requirements critical to cyber resilience.

(16) Deliver all test data, reports, and documentation to the project or program managed repositories. Manage all test data, reports, and other documentation in accordance with DoDI 5015.02.

e. Lead OT&E Organization.

The DoW Component designated lead OT&E organization (e.g., operational test agency or operational test organization) will support the CyWG to maximize government integrated cyber T&E and optimize cyber DT&E planning to support assessments of operational effectiveness and suitability, as applicable.

SECTION 4: CYBER DT&E ITERATIVE PROCESS

4.1. OVERVIEW.

As depicted in Figure 1, cyber DT&E is an iterative process of planning, preparing, executing, evaluating, and reporting.

Figure 1. Cyber DT&E Process

4.2. ITERATIVE PLANNING FOR CYBER DT&E.

The CyWG is responsible for these iterative planning activities.

a. CyWG Cyber DT&E Strategy Scoping.

The CyWG begins cyber DT&E strategy scoping as early as possible for any system development, including S&T and prototype development.

(1) Examine and Advise on Cyber Requirements.

The CyWG will:

(a) Participate in stakeholder requirements development to ensure requirements are measurable and testable.

(b) Review available artifacts and system documentation to identify stated or derived cyber performance requirements and mission context before developing or updating the cyber DT&E inputs to the TEMP or T&E strategy.

(c) Advise the system engineering team on identified weaknesses or gaps in operational resilience in cyberspace requirements.

(d) Provide recommended changes for cyber performance requirements to the system engineering team if cyber performance requirements are not measurable or testable.

(e) As appropriate, advise on technical strategies to prevent, detect, contain, mitigate or eliminate, and recover from the loss of system capabilities (e.g., strategies associated with implementing the DoD Zero Trust Reference Architecture and the DoD Cybersecurity Reference Architecture).

(f) Map the cyber technical performance requirements in the TEMP or T&E strategy to test events in the IDSK aligned to the appropriate decisions.

(2) Examine Current Threat Assessments.

The CyWG will:

(a) Request support from and collaborate with the appropriate intelligence resource (e.g., DoW and Military Service intelligence organizations, program intelligence liaisons) to conduct system threat analyses.

(b) Use the latest system-relevant intelligence product(s) as the threat, system, operational environment, or mission evolves to inform the TEMP or T&E strategy, MBCRAs, and cyber DT&E plans.

(3) Characterize Attack Surface.

The CyWG will:

(a) Examine evolving documentation, cyber requirements, and system artifacts, system developer (contractor) and operational processes, documentation of system developer processes in the hardware and software supply chains, system components, technologies, and interfaces.

(b) Use Table 1 to inform the attack surface characterization.

(c) Identify, assess, and document potential weaknesses that could affect technical, functional, and operational performance and generate an attack surface diagram.

(d) Use the attack surface as input to the next MBCRA and to inform the TEMP or T&E strategy and cyber T&E plans.

(4) Support Criticality Analysis.

The CyWG will:

(a) Coordinate with the system security engineering team to support initial and updated end-to-end mission and functional decomposition and analyses using threat TTPs and prior MBCRA and cyber DT&E results. Ensure the analysis identifies MRT-C in support of mission assurance.

(b) Iteratively review and update criticality analysis as the threat, system, operational environment, or mission evolves.

(c) Use the criticality analysis output to revisit and update the attack surface characterization.

(5) MBCRAs.

A MBCRA is an analytical iterative process to identify, estimate, assess, and prioritize risks to DoW operational missions resulting from cyber events. The DoD Cyber Table Top Guide provides one example of a MBCRA methodology. The CyWG will ensure iterative or updated MBCRA reports:

(a) Support test design, scoping, and prioritizing the testing of subcomponents, components, subsystems, systems, and interfaces, based on projected impacts from cyber effects.

(b) Inform, and not limit, future testing.

(c) Inform cyber requirements, engineering, programmatic, risk management, test, defense planning, and operational utilization activities and decisions.

(d) Focus on cyberspace threats to operational missions the system will support.

(e) Enable further characterizing the attack surface and risks, exploring elements in Table 1, the MRT-C, mission or safety critical functions, components, and interfaces of the system.

(f) As depicted in Figure 2, use all available information on operational mission(s), system(s), and threat information to inform MBCRAs, including, at a minimum, these inputs:

1. Latest system and criticality analysis details (e.g., mission, functions, decomposed mission and safety critical functions, architectures, components (software, hardware, and firmware), data flows, protocols, interfaces, mitigations and protections, maintenance processes), with identified MRT-C.

2. Current threat intelligence, including the adversary's means or capability, opportunity or tactics, and motive or intent.

3. Current attack surface characterization.

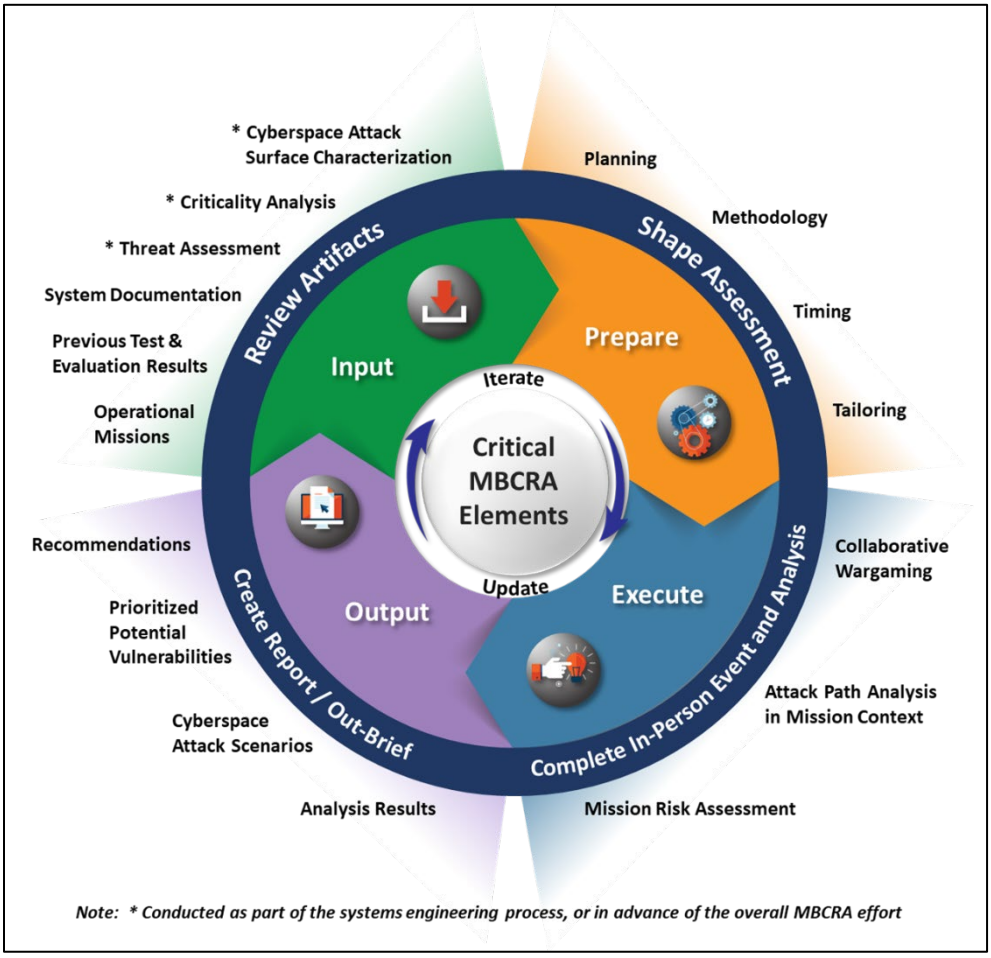
4. A listing and analysis of known vulnerabilities (including BOM analysis).

5. Any available previous cyber risk assessments, cyber test results, and DoD RMF plan of action and milestones data.

6. Incident response plan.

7. Selected system mission(s) and mission scenario(s).

Figure 2. MBCRA Elements



(g) Use methodologies that include the minimum activities depicted in Figure 2:

1. Attack path and system design analysis to identify potential for faults and exploits that could impact the mission(s).

2. Risk assessments of faults and exploits for selected mission(s) and mission scenario(s).

3. A process that incorporates collaborative wargaming using defensive and adversarial cyber representatives, operators, and system design engineers. If available, include defenders, developers, intelligence community representatives, and maintainers.

(h) Provide reports detailing the analysis results including detailed cyberspace attack scenarios, prioritized potential vulnerabilities, and recommendations for remedies, mitigations, and testing, as depicted in Figure 2.

(i) Support acquisition decisions throughout the system's life cycle in response to changes in the system design, environment, and threats.

(6) Use Prior Test Results.

The CyWG will:

(a) Use all available prior cyber or non-cyber test results on the current or similar systems or versions to verify mitigations or remediation and inform scoping and upcoming test design while considering test coverage, risks, threats, critical functionality, resources, and priorities.

(b) Prior testing results inform decisions regarding engineering, remediation, mitigation, maintenance, sustainment, and defender processes.

b. CyWG Input to System Developer Contract Requirements.

The early TEMP or T&E strategy, along with the scoping efforts outlined in Paragraph 4.2.a of this issuance, will guide the development of cyber DT&E requirements for RFPs and acquisition contracts. These requirements will be specified through contract data requirements lists, data item descriptions, and clauses aligned with the Federal Acquisition Regulation, the Defense Federal Acquisition Regulation Supplement, or other applicable agreements. The CyWG works with the contracting officer to include:

(1) Provisions ensuring:

(a) Iterative and recursive cyber T&E activities, to include regression testing, throughout the system development life cycle, including on prototypes, before government acceptance cyber T&E.

(b) Testing to assess the impact of potential cyber threats alongside non-cyber evaluations.

(c) System development contractors performing cyber DT&E are qualified in accordance with the DoDD 8140.01.

(d) Cyber T&E accounts for safety, hazard, and loss considerations when testing cyber physical systems.

(e) Inclusion of the CyWG as observers of contractor cyber DT&E events and design reviews.

(f) Government physical access to contractor facilities, supplier and systems development environments, cloud infrastructure, and the physical hardware supporting infrastructure (e.g., servers, routers, switches, and other equipment).

(g) Government access to contractor test labs and contractor-developed digital twins, models, or simulations of systems and their components to support government acceptance cyber T&E.

(h) Contractor support of government-led cyber T&E planning activities including attack surface analysis, MBCRAs, and government use of contractor systems integration labs.

(i) Contractor support for government cyber T&E.

(j) Support for government-led cyber T&E in contractor-owned, contractor-operated facilities with contractor-provided tools and resources or when contractor outsourcing circumstances require similar provisions for government-led cyber T&E activities.

(k) Contractor mitigation or remediation responsibilities in the case of government rejection of the system if government acceptance testing identifies accessible and exploitable vulnerabilities or deficiencies before government acceptance of the system during testing and throughout the development process.

(l) If applicable, software reverse engineering data rights or delivery of source code.

(2) Delivery of:

(a) Current contractor data used to inform the system's attack surface analysis, including security strategies, plans, evaluations, and activities related to protecting and defending the digital engineering, development, manufacturing, and test environments, processes, and tools, including software pipelines.

(b) Data on supply chain illumination.

(c) System design information.

(d) Digital twins, digital models, or cyber test assets.

(e) The cyber requirement verification traceability matrix, in accordance with the DoD Systems Engineering Plan Outline, and data demonstrating technical cybersecurity and cyber resilience performance requirements.

(f) Test plans aligned to Table 3 during system engineering design and development, before formalized testing begins.

(g) Contractor cyber test data and reports aligned to Table 4.

(h) Security verification data.

(i) Test-based evidence that corrective actions sufficiently remediate or mitigate mission impacting vulnerabilities and deficiencies in accordance with DoDI 8531.01.

c. Cyber DT&E Iterative Input to the TEMP or T&E Strategy.

In accordance with DoDI 5000.89, the TEMP or T&E strategy will:

(1) Document cyber DT&E plans which enable the cyber DT&E process to respond to changing cyberspace threats.

(2) Document cyber DT&E plans based on previous T&E results, and aligning with the latest attack surface analysis, focusing on critical functions and the MRT-C, using relevant threat information, and maximizing the use of:

(a) Available M&S.

(b) Automated cyber analytics.

(c) Cyber testing infrastructures, tools, and other capabilities.

(d) Other available digital approaches (e.g., model-based systems engineering, cyber analytic tools) to scope and perform cyber DT&E activities.

(3) Include the plan and resourcing for MBCRAs and testing of MBCRA findings.

(4) Document measurability, testability, and traceability of cyber requirements to mission and safety critical functions identified as part of the mission assurance construct in accordance with DoDI 3020.45 and system criticality analysis pursuant to DoDIs 5000.83 and 5200.44.

(5) Outline the planned cyber DT&E events in the IDSK, using scoping activities in Paragraph 4.2.a., and a variety of test types from Table 2. In coordination with the CyWG, the T&E WIPT, or ITT as appropriate, will update the IDSK throughout the system's life cycle to support new IDSK decisions.

(6) Summarize the cyber DT&E requirements the system developer (contractor) must perform and the approach to assess the contractor's tests, data, results, and effectiveness of remediation and mitigation implementation.

(7) Summarize the overarching security verification approach, including tools, frequency, remediation processes and plans, and access to the data repository.

(8) Describe the process for documenting and tracking vulnerabilities and deficiencies throughout the acquisition life cycle in the existing deficiency management program.

(9) Document plans for regression testing, including confirming the effectiveness of vulnerability remediation and mitigation implementation.

(10) Capture the funding, resources, staffing, and schedule, including any related limitations and risks, to accomplish cyber DT&E. Specifically, address:

(a) Any required low-supply but high-demand cyber developmental test teams and physical assets (e.g., labs, facilities, test assets, T&E tools, and operational platforms).

(b) Any long-lead test environments (e.g., labs, cyber test ranges, representative interfaces, and cyber test networks, including operationally representative or actual operational networks and supporting systems) needed.

4.3. PREPARING FOR CYBER DT&E.

The responsible cyber DT&E team will:

a. Develop Cyber DT&E Plans.

All system developer (contractor) and government cyber DT&E events require approved cyber DT&E plans. System developer (contractor) and government cyber DT&E plans will:

(1) Document the test plan, test scenarios, and assumptions for planned tests at the subcomponent, component, subsystem, and system level.

(2) Not exclude components or systems due to unmitigated weaknesses or vulnerabilities or knowledge the component or system will fail the test.

(3) Use the latest MBCRA results.

(4) Specify cyber developmental test objectives and plans to measure and evaluate technical cyber resilience requirements in a mission context.

(5) Define the extent to which the responsible cyber DT&E team is authorized to operate and move freely within the system under test, adapting to emerging situations during testing, including their ability to explore system under test behaviors, identify vulnerabilities, and gather relevant insights, except where safety, legal, regulatory, or other authoritative constraints impose limitations.

(6) Use scientific testing and analysis techniques to evaluate technical performance in cyberspace.

(7) Specify the mission-based scenarios the responsible cyber DT&E team will use to evaluate the potential impacts on mission execution, system performance, or cyber resilience effectiveness caused by cyber vulnerabilities, adversarial actions, or system faults.

(8) Incorporate all relevant TTPs used by threat actors, as identified from open source, commercial, and government intelligence community sources. Ensure the test accounts for an adversary's most likely and most dangerous courses of action in the most realistic environment(s) available.

(9) Specify all relevant systems under test, systems supporting the test, interfacing systems, and network architectures appropriate to successfully support planned tests.

(10) Include any missed or deferred system components, functionalities, or requirements that were not previously tested, as the system matures across the acquisition life cycle, and as the test conditions' operational realism increases.

(11) Use cyber ranges instead of live operational systems when the CyWG identifies potential safety risks, unacceptable mission impacts, or concerns about the loss of system functionality, data, or operational capability.

(12) Segment test events as necessary and allocate resources to generate and gather data from the separate test events to support comprehensive data collection across attack kill chain steps and the system's life cycle as required.

(a) Integrate software assurance test results and M&S data when full system testing of the entire operational capability or an attack kill chain is not feasible due to significant risks or safety concerns.

(b) Ensure the overall test effort collects the data required to evaluate the system's performance, cybersecurity, and cyber resilience requirements as if the data were derived from a single, unified test event.

(13) Incorporate varying test types from Table 2 to ensure comprehensive coverage of the system's cybersecurity and cyber resilience requirements.

(14) Include the primary data or information from Table 3.

b. Prepare for Cyber DT&E Events.

Cyber DT&E event preparation includes:

(1) Developing or identifying cyber DT&E tools and data resources.

(2) Identifying the required cyber test instrumentation, data collection plan, test asset, interfaces, or infrastructure.

(3) Scheduling cyber test facilities.

(4) Establishing connection agreements for distributed cyber tests.

(5) Confirming, as required, connectivity of networks or communication paths external to the system under test along with the necessary permissions and accesses for the responsible cyber DT&E team to operate on these external networks.

(6) Confirming funding, staffing, and support resources for the upcoming cyber test events.

(7) Reviewing all prior cyber test reports.

(8) Employing all relevant security classification guides to help ensure appropriate handling, processing, and custody of all test data, analysis, and reporting.

(9) Conducting prior coordination and verification testing to ensure cyber T&E tools do not cause unintended harm to the system under test unless the planned test asset or environment supports destructive tactics (e.g., the use of a cyber range, virtualization, digital twins, or model-based testing) or is a destructive test event.

c. Conduct Cyber DT&E Readiness Reviews.

(1) Lead DT&E organizations will include cyber DT&E plans in government DT&E readiness review processes. The cyber DT&E readiness review will include:

(a) A full evaluation of the rules of engagement agreement between the system owner and the responsible cyber DT&E team, including the approved target strike and do not strike lists.

(b) Consideration of testable controls from the security assessment plan to complement the DoD RMF security control assessment (e.g., finding password requirements fail to meet the stated policy), if applicable.

(c) Confirmation of DoD RMF authorization, as required.

(d) Confirmation test assets do not introduce unplanned risks to the system under test.

(2) The responsible cyber DT&E team will not modify cyber DT&E plans due to knowledge the component or system will fail the test.

4.4. EXECUTING CYBER DT&E.

a. The responsible cyber DT&E teams will execute:

(1) Cyber developmental test events in accordance with DoDI 5000.89 and the CDT or T&E lead's approved test plans.

(2) All planned and prepared tests on all planned systems regardless of whether the systems have known unmitigated vulnerabilities or weaknesses.

b. The responsible cyber DT&E teams will record any deviations from approved test plans during test execution, the new conditions under which the responsible cyber DT&E teams collected the data, and the reasons for the deviations to incorporate in the report.

4.5. EVALUATING CYBER DEVELOPMENTAL TEST DATA.

The responsible cyber DT&E teams will:

a. Implement the evaluation procedures in accordance with DoDI 5000.89.

b. Study system developer (contractor) delivered test reports.

c. Correlate all findings with evidence and non-cyber test results.

d. Evaluate test data and measurements against cyber performance requirements.

e. Evaluate the status of previously discovered deficiencies.

4.6. REPORTING CYBER DT&E RESULTS.

a. The responsible cyber DT&E teams will report on cyber DT&E results in accordance with DoDI 5000.89.

b. System developer (contractor) cyber T&E and government cyber DT&E reports will incorporate the applicable information outlined in Table 4.

c. Cyber DT&E reports will:

(1) Include recommendations on how to improve the system's cybersecurity and operational resilience in cyberspace risk postures.

(2) Comply with all applicable security classification guide requirements for marking and handling test data and reports.

d. The responsible cyber DT&E teams will store copies of all cyber test reports and manage all reports in accordance with DoDI 5015.02.

e. The responsible cyber DT&E teams will include identified vulnerabilities or other deficiencies in the Joint Deficiency Reporting System or other DoW Component deficiency reporting database.

APPENDIX 4A: DETAILED CYBER DT&E PLANNING AND REPORTING REQUIREMENTS

Table 1. 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 (e.g., Machine Learning, Deep Learning, Natural Language Processing, Robotics) and Big Data Applications	• Consider training and model parameter data poisoning. • Consider susceptibility of altered analytics and other attacks. • Consider model extraction attacks.
Commercial Cloud Environments and Cloud Services	• Consider access to system developer (contractor) test data and conducting cyber testing of cloud service infrastructure and implementation. • Consider the physical and logical components of the hosting cloud or center for hosted systems. • Consider how the cloud architecture interfaces with the system and government networks. • Consider cloud service level agreement(s) to determine service speed and productivity, 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 system and monitor defense industrial base breaches. • Evaluate cyber supply chain risk management assessments for hardware and software components and risk mitigation actions.
DoW Infrastructure and Enterprise Services	• Evaluate the system's dependencies on and interfaces with external infrastructure and services. • Evaluate trust relationships, authorizations, and confidence in implementation of zero trust, as applicable.
Electromagnetic Spectrum	• Identify and evaluate any system exposures to cyberspace attacks in and through the electromagnetic spectrum. • Assess and inform planned electromagnetic spectrum testing, including key radio frequencies, data links, and other spectrum pathways. • Address how to use testing to support T&E of systems in complex electromagnetic spectrum to accomplish or defend against cyber exploitation.

Table 1. Examples of Evolving Attack Surface Elements, Continued

Attack Surface Elements	Actions
Inter- and Intra-System Architecture Network Interfaces	• Evaluate the dependencies on interfaces and application program 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 DoW networks) networks local to the system, and non-IP networks (e.g., Military Handbook MIL-HDBK-1553A). • Evaluate the infrastructure dependencies, designed in resilience measures, and validate contingency planning, continuity of operations, and disaster recovery planning. • Validate the adequacy of the critical infrastructure protection plan. • Evaluate the transition points from IP to control systems' protocols for opportunities to detect intrusions.
Interfaces with Interagency	• Evaluate interface risks, including application program interfaces, using cyberspace 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 Cybersecurity and Infrastructure Security Agency). Note: Commercial threat information can be used as cueing for collaboration with the intelligence community.
Real-Time, Safety-Critical Systems (e.g., Industrial Control Systems, Supervisory Control, and Data Acquisition)	• Evaluate potential test approaches, making use of information from expert sources (e.g., maintainers, operators, systems engineers). • Identify 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 TTPs for the DoW.
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 system's PPP, supply chain risk management plan, program protection implementation plan, and similar sources to help inform testing scope via fully sourced criticality, interdependence, and operational considerations. • Review contractual cyber DT&E requirements (i.e., test procedures and resources) for supply chain testing. • Evaluate software, software libraries, firmware, hardware, and BOMs to determine provenance. • Evaluate if the 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 exposures in the operational and technical requirements, critical functions, and the proposed or anticipated architecture or implementation information (or architectural information from prototypes, or surrogate systems, if required).

Table 2. Cyber Developmental Test Types

Test Types	Description	Test Considerations
Architectural Vulnerability Assessment	Examines network and system architecture attributes that may introduce attack paths to critical cyber assets.	Examine system developer (contractor) technical design documentation. Investigate inherent architectural vulnerabilities. Examine trust relationships external to the system and critical data exchanges.
Bug Bounty (Classified or Unclassified)	A crowdsourcing effort to identify vulnerabilities in a system (e.g., software or hardware component, sub system, system, system-of-systems).	Unclassified: Plan, resource, and coordinate with a public bug bounty provider. Classified: Plan and coordinate with Office of the USW(R&E), Office of Developmental Test, Evaluation, and Assessments.
Cloud Testing	Performing the applicable cyber DT&E activities within this issuance and this table to cloud service offerings under acquisition of services (e.g., software as a service, platform as a service, infrastructure as a service, and hybrid solutions).	Understand shared security model, contract vehicle, or service level agreements, roles, and responsibilities, including test roles. Understand all interfaces to other systems, system-level users, identity and access management, privacy controls, multi-cloud configurations, and authorization mechanisms.
Concurrent Cyber and Non-cyber Testing	Integrated adversarial cyber testing using threat representative tactics and techniques with other testing including functional performance, interoperability, and other non-functional operational and support requirements (e.g., reliability, availability, maintainability, supportability).	Consider safety. Consider impact on other functional test objectives. Use MBCRA findings. Ensure responsible cyber DT&E team has well-defined rules of engagement for any destructive or abusive testing.
Control Testing	Verifies cybersecurity functionality to ensure security controls and countermeasures are working as intended in a mission context.	Test security controls and countermeasures in a mission context before IATT. Verify system developer (contractor) cyber DT&E results.
Critical Infrastructure Assessment	Targets the system under test's logical dependencies on critical infrastructure (e.g., power, water) to assess if the incapacity or destruction of such systems and assets would have a debilitating impact on the system under test's operational capability.	An infrastructure is logically dependent if its state of operations depends on the state of another infrastructure via a mechanism that is not a physical, cyber, or geographic connection. Logical dependency is attributable to human decisions and actions and is not the result of physical or cyber processes.
Cyber-Electromagnetic Spectrum Operations Testing (EMSO)	Cyber-EMSO implications of new, existing, or modified waveforms on mission operations.	Testing should consider waveforms and radio frequency apertures as threat vectors. Common tools include spectrum analyzers, software defined radios, high gain antennas, and oscilloscopes.
Cyberspace Kill Chain Testing	Deliberate tests using a planned scenario maneuvering through the kill chain to create a planned effect.	Safety; documenting indicators of compromise for improving detection and response.

Table 2. Cyber Developmental Test Types, Continued

Test Types	Description	Test Considerations
Incident Response Testing	Tests the incident response capability for the system to determine the incident response effectiveness.	Use checklists, incident response plans, walk-throughs, tabletop exercises, or simulations. Testing may occur during logistics demonstrations.
Interface Testing	Assesses the interaction and exploitability risks between interacting systems or applications.	Check for authentication and encryption, man-in-the-middle, authentication bypass, denial of service, misuse, tunneling, user interfaces, exploitable misconfigurations, and resulting measurable performance impacts.
MBCRA Verification	Verifies scenarios and evaluates mission impacts of vulnerabilities explored during MBCRAs.	Test suspected exploitable weaknesses and vulnerabilities to validate MBCRA findings. Evaluate system performance during attack using safe test environments.
Network Vulnerability Assessment	Targets system's enclave network boundary, internal networks, system interfaces, and network security components.	Test for misconfigured devices and nonfunctional protections at the network level (e.g., network segmentation and firewalling).
Non-IP Device and Component Testing	Verify required security and resilience performance requirements of embedded systems, real time operating systems, protocols, and platforms of systems at the supply chain and hardware levels.	Conduct MBCRAs to scope. Test for accessibility to unnecessary features. Conduct interface testing to examine authentication and validation of incoming data and security against unauthenticated receivers. Common tools for hardware data extraction include soldering equipment, multimeters, universal serial bus-to-serial adapters, and logic analyzers.
Penetration Testing or Exploitation Analysis	Authorized, simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.	Target key cybersecurity and operational resilience in cyberspace assets supporting mission-essential functions for penetration and exploitation.
Platform and Component Hardening Verification	Verifies security of components and platforms of systems at the supply chain and hardware levels.	Provides input to the system engineering process. Assess patching processes for components to address vulnerabilities that occur after deployment. Assess anti-tamper measures.
Purple Team Testing	Tests that include both adversarial and cooperative tactics. Informs the processes and procedures required to prevent, detect, contain, mitigate or eliminate, and recover mission or safety critical capabilities.	Requires deconfliction of cooperative and adversarial activities to reduce negative impacts of tests and to clarify the system under test's defensive capabilities.
Recoverability Testing or Continuity of Operations Testing	Verifies actions taken during or after an incident or event to restore functions and capability to fully operational states in mission relevant timelines.	Ability to measure each aspect of recovery, failover, and restoration. Testing may occur during logistics demonstrations.
Resilience Testing	Ensures the mission or safety critical functions are resilient to adverse cyber incidents.	Requires measurable and testable requirements for prevent, mitigate, and recover.

Table 2. Cyber Developmental Test Types, Continued

Test Types	Description	Test Considerations
Reverse Engineering	Using a disassembler, a debugger, and a de-compiler to examine low-level assembly or byte-code instructions.	Intellectual property restrictions.
Security Technical Implementation Guide Testing	Rigorous component scanning that includes evaluating scan results, eliminating false positives, and performing manual checks.	Test each critical cybersecurity asset and adjudicate all confirmed findings. Use multiple scanning tools to cross-validate vulnerability findings. Note: security technical implementation guidance verification during DT&E provides input to authorizing official and does not replace RMF security control assessments.
Software Assurance Testing	Identifies and eliminates software errors and vulnerabilities in critical components; system developer (contractor) T&E is the earliest instance of software testing.	Perform software security verification using requirements specified in the PPP. Address three areas: • Software development environment. • Software development processes. • System operational software.
Software Factory Testing	Penetration testing of the software factory people, processes, environments, application program interfaces, and tools.	Government testing of government-owned factories. Software developer contractor testing of contractor-owned factories.
Supply Chain Testing	Targeted cyber tests informed by supply chain risk management, mission relevant terrain in cyberspace, or criticality analysis.	Focus on the critical parts and suppliers which could have the greatest impact on the system's mission and provide easy adversarial access. Obtain information on the provenance, pedigree, history, and role of system parts (if possible) to support credible, risk-based screening and attack response.
System Misuse and Abuse Testing	Examines how systems are used in unplanned, unintended, or unexpected ways.	Use misuse and abuse scenarios to guide testing with a mission context. An understanding of predicted threats provides input into system abuse scenarios.
Threat Hunting	Using threat intelligence to proactively search for advanced threats and previously unknown, non-remediated threats within the system's software, firmware, compliers, and development pipelines.	Research the threat's TTPs. Simulate the most likely threat steps. Assemble team with relevant skills and tools. Plan to reverse engineer software. Environment and timeline for automated fuzzing to deliver hidden triggers, and ability to instrument the system to detect effects.
Vulnerability Assessment	Systematic examination of a system under test to determine the adequacy of security and resilience functions, identify deficiencies, provide data from which to predict the effectiveness of proposed security and resilience functions, and confirm the adequacy of such functions after implementation.	Informs next cyber testing (e.g., penetration testing, kill chain testing, resilience testing, testing non-IP systems) and related protocols. Cover the full attack surface and interfaces, commercial off the shelf products, software and hardware assurance, network-based assessments, database assessments, wireless network exposures, supply chain risks.

Table 3. Cyber Developmental Test Plan Data

Section	Description
System What is being tested?	Describe the architecture of the system(s), system-of-systems, families of systems, or platform of systems, mission context, and provide detailed network diagrams.
Test Environment Where is the test being done?	Describe conditions, assumptions, and limitations affecting overall test conduct. Describe the cyber environment for the system.
Time and Resources When and who, using what?	Provide the schedule of test events, resource, and tools.
Vulnerability Identification, Documentation, Tracking, Scoring, and Retesting How?	Describe how the test team will use results from prior security verification tests and conduct the test activities to gather the required data. Describe the process to identify, document, track, and determine severity of vulnerabilities during the test.
Cyber Test Techniques How?	Describe how the test team will conduct the test activities and gather required data. Describe the anticipated test risks, limitations, and risk mitigations. Describe the requirements and test measures the test will verify. Describe what data is being collected and how the test team will conduct the test activities to gather required data. Describe planned integrated tests. Describe planned regression tests.
Defensive Capabilities How?	Describe how during or after an attack the test will collect the observations and actions of the operators, the system's ability to prevent mission loss, detect effects, contain incidents, mitigate losses or eliminate incidents, and recover or adapt. Describe metrics and expected defensive cyber tools.
Threat Representative Offensive Capabilities How?	Describe plans for attack surface assessments (e.g., interfaces, critical infrastructure, supply chain, insider, outsider, EMSO, physical penetration). Describe planned offensive techniques, tools, and MBCRA verification scenarios. Describe planned supply chain cyber test scenarios. Describe planned targeted mission or safety critical data, mission or safety critical functions and expected system behaviors and impacts. Describe the planned emulated threat environment.

Table 4. Cyber Developmental Test Reporting Data

Section	Information
Test Conduct (test execution context)	Schedule, organizations, facilities, limitations or constraints, and deviations from the plan.
System Configuration (contextual data about actual system configuration, as tested)	Versions, configurations, addresses, data flows, interfaces, protections, differences from expected or planned architectures and configurations.
Cyberspace Attack Scenarios (contextual data describing the threat)	Describe adversarial techniques, activities, threat representation level, evidence of success, use of white cards and impacts of all attack scenarios.
Supply Chain (supply side context)	Describe unexpected system behaviors, identified areas of weakness in developer processes, tools, environments, and tools, open source vulnerabilities, checksum variances, effects of environmental triggers, and behaviors associated with supply chain white cards. Observed anomalies in system, subsystem, component, or subcomponent behaviors.
Vulnerability and Exposure Identification – Scans	Describe identified vulnerabilities and patching status or plans, and severity scores.
Vulnerability and Exposure Exploitation	Describe results of vulnerability exploitation, (e.g., access attained, detections) and exploitation techniques or tools required.
Integrated Cyber EMSO Testing	Describe how the electromagnetic spectrum did or could enable or hinder aggressive cyber activities.
Operational Mission Effects including Force Protection	Report measured, observed, anticipated, or estimated effects of exploitation.
Prevent (Identify, Protect)	Describe the inherent (baseline truth) and inherited (deltas) cyber defenses, cyber actions prevented and means of prevention (success), the mechanism used to detect or discover the actions (e.g., cyber defender, automated notifications or monitoring), and cyber actions not prevented (failures) requiring mitigation, containment, elimination, or recovery.
Mitigate (Detect, Contain, Eliminate, System Monitoring)	Describe evidence, measurement, techniques, and effectiveness of detections, containments, elimination of incidents, and system monitoring capabilities.
Mitigate (System Response Actions)	Describe evidence, measurement, techniques, and effectiveness of system or operator response capabilities.
Recover or Adapt (System or Operator Recovery or Adaptation and Restoration Actions)	Describe evidence, measurement, techniques, extent (full or decremented) and effectiveness of anticipated (or actual) restoration (recovery of affected system functions) capabilities.

SECTION 5: CYBER DT&E FOR ADAPTIVE ACQUISITION FRAMEWORK PATHWAYS

5.1. GENERAL.

Each of the adaptive acquisition framework pathways, depicted in Figure 3, requires planning and conducting both system developer (contractor) cyber DT&E and government cyber DT&E events. The CyWG helps the PM customize the program's cyber DT&E activities in accordance with Sections 3 and 4 of this issuance for the chosen acquisition pathway. Paragraphs 5.2. through 5.8. of this issuance align the major cyber DT&E activities to specific cyber DT&E stages of the corresponding pathway, as shown in the tables and figures in this section. Tables 5 through 10 distinguish between where:

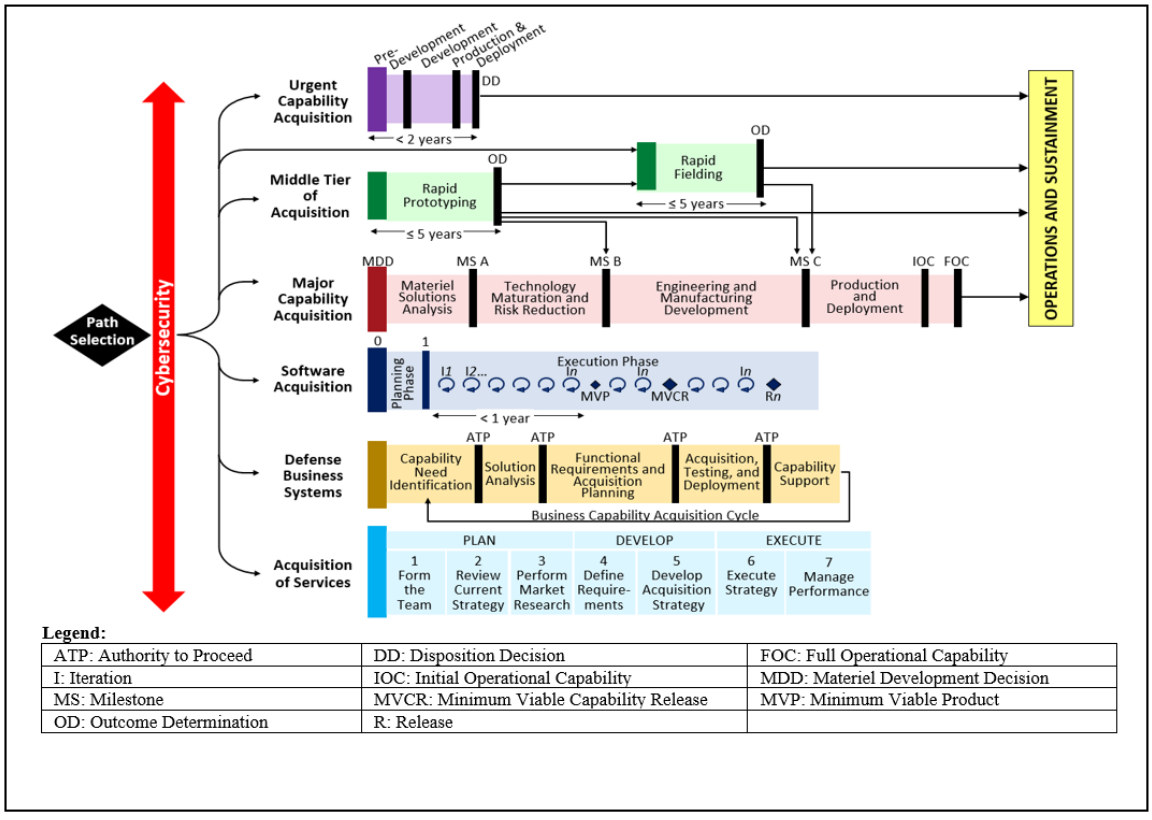
a. The stated program activity must be fully performed (●).

b. The activity should be repeated or could be a program-specific option (○).

c. Prior activity results must be updated (↻).

d. The program activities of plan, prepare, execute, evaluate, and report occur using colored rows based on activity colors in Figure 1.

Figure 3. Adaptive Acquisition Framework



Legend:

ATP: Authority to Proceed	DD: Disposition Decision	FOC: Full Operational Capability
I: Iteration	IOC: Initial Operational Capability	MDD: Materiel Development Decision
MS: Milestone	MVCR: Minimum Viable Capability Release	MVP: Minimum Viable Product
OD: Outcome Determination	R: Release	

5.2. URGENT CAPABILITY ACQUISITION (UCA) PATHWAY.

a. Table 5 outlines program activities in four stages for the UCA pathway:

(1) Pre-development.

(2) Development.

(3) Production and deployment.

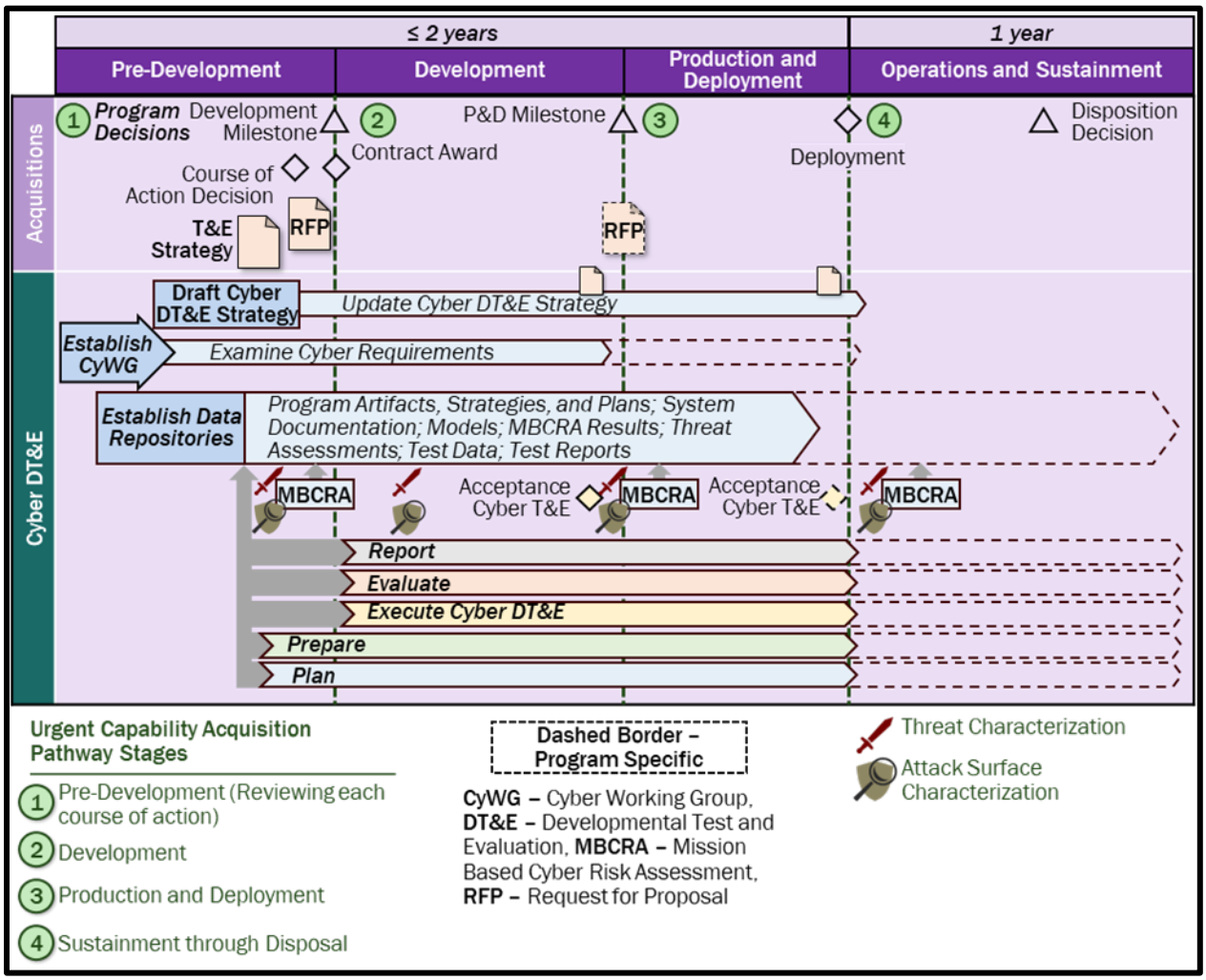
(4) Sustainment through disposal.

b. Figure 4 provides a sample of cyber DT&E activities for the UCA pathway schedule, based on Table 5.

Table 5. UCA Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3	4
Establish and charter the CyWG	●			
Examine and advise on cyber requirements	●	●	○	○
Examine threat assessments and characterize attack surface	●	●	●	●
Support criticality and MRT-C analysis	●	↻	↻	○
Conduct or update MBCRA	●		○	○
Develop or update cyber DT&E strategy	●	↻	↻	↻
Determine test infrastructure, tools, and data requirements	●	↻	↻	↻
Plan resources and schedule government cyber DT&E	●	●	↻	↻
Include cyber DT&E requirements in each RFP and contract	●	○		
Review system developer (contractor) or government development and test environment, processes, and tools		●	○	
Analyze existing or known vulnerabilities		●	●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received		●	○	
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing		●	●	●
Conduct test readiness reviews		●	●	●
Execute security verification throughout the system's life cycle		●	●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system		●	●	
Execute planned government acceptance cyber T&E		●	○	
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events			●	
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies		●	●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01		●	●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●	●
Plan and update sustainment cyber DT&E activities and frequency			●	↻

Figure 4. Sample Cyber DT&E Activities for the UCA Pathway



5.3. MIDDLE TIER OF ACQUISITION (MTA) PATHWAY.

a. The CyWG performs the same cyber DT&E activities for both rapid prototyping and rapid fielding. Table 6 outlines program activities in three stages for the MTA pathway:

(1) Planning.

(2) Execution.

(3) Transition.

b. Figures 5 and 6 provide a sample of cyber DT&E activities for the MTA pathway schedules, based on Table 6.

Table 6. MTA Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3
Establish and charter the CyWG	●		
Examine and advise on cyber requirements	●	●	●
Examine threat assessments and characterize attack surface	●	●	●
Support criticality and MRT-C analysis	●	↻	○
Conduct or update MBCRA	●	↻	○
Develop or update cyber DT&E strategy	●	↻	↻
Determine test infrastructure, tools, and data requirements	●	↻	↻
Plan resources and schedule government cyber DT&E		●	↻
Include cyber DT&E requirements in each RFP and contract	●		○
Review system developer (contractor) or government development and test environment, processes, and tools		●	○
Analyze existing or known vulnerabilities		●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received		●	○
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing		●	●
Conduct test readiness reviews		●	●
Execute security verification throughout the system's life cycle	●	●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system		●	●
Execute planned government acceptance cyber T&E		●	
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events		●	●
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies		●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01		●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●
Plan and update sustainment cyber DT&E activities and frequency			●

Figure 5. Sample Cyber DT&E Activities for the MTA Rapid Prototyping Pathway

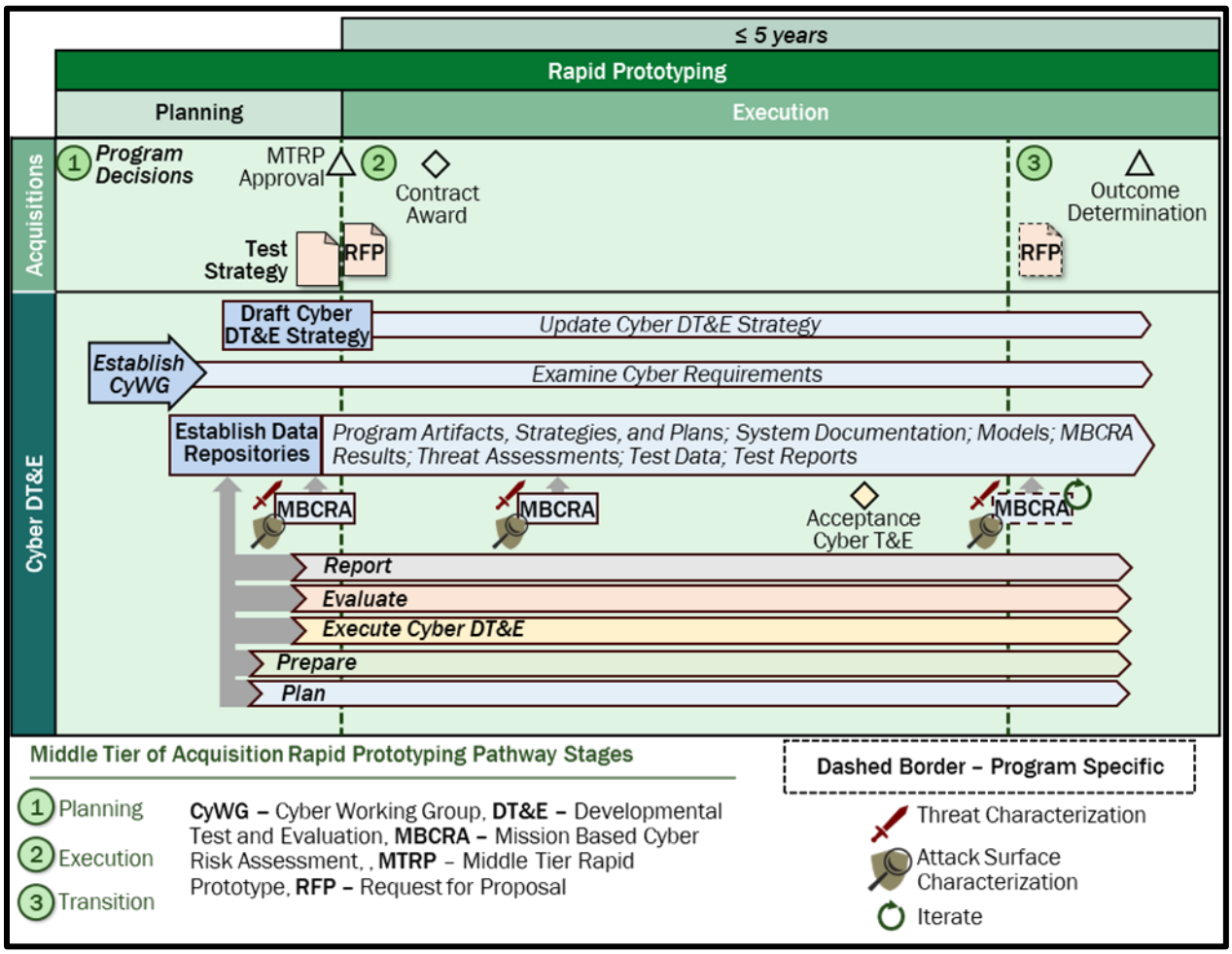
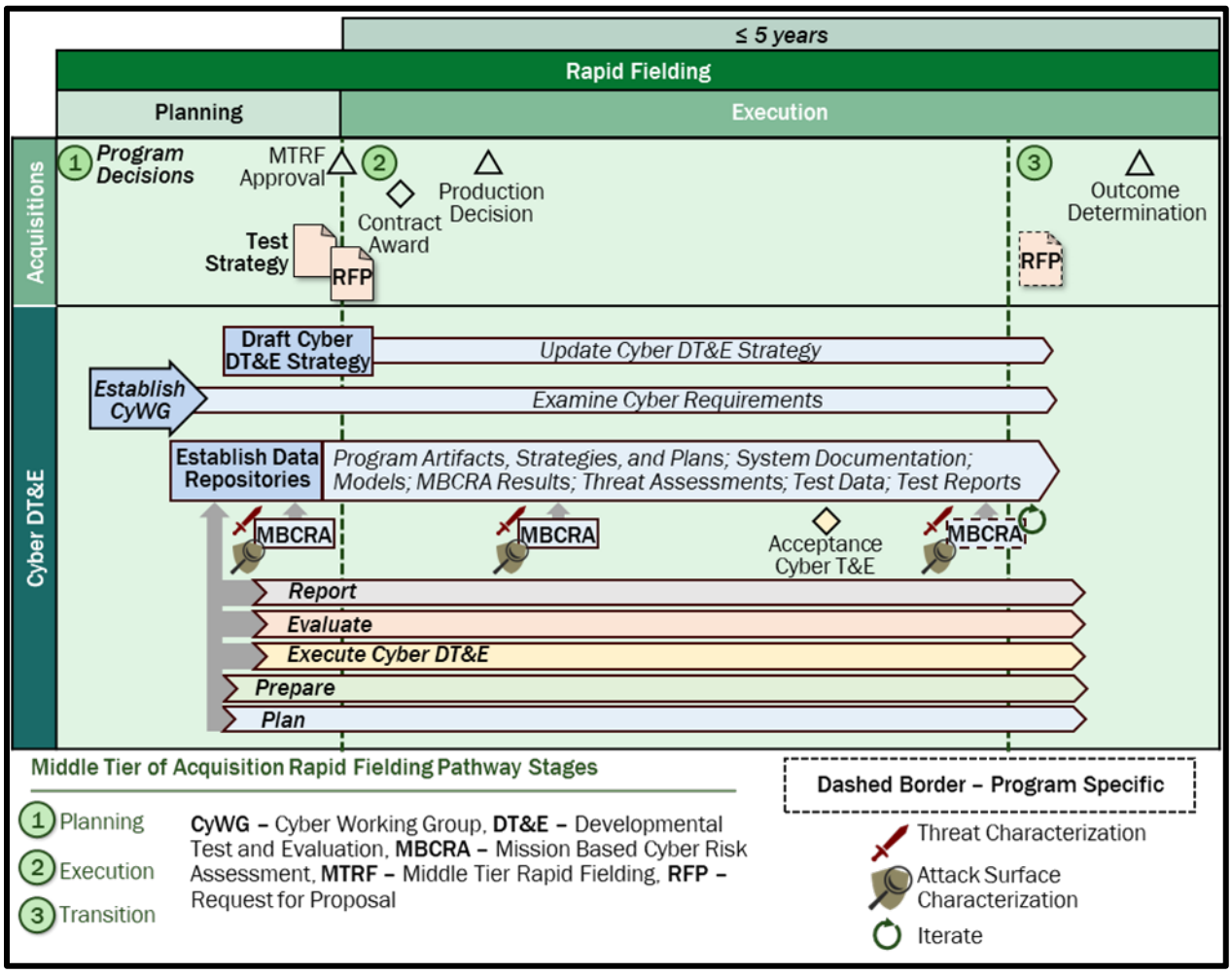


Figure 6. Sample Cyber DT&E Activities for the MTA Rapid Fielding Pathway



5.4. MAJOR CAPABILITY ACQUISITION (MCA) PATHWAY.

a. Table 7 outlines program activities in six stages for the MCA pathway:

(1) Up to Pre-Milestone A.

(2) Milestone A through Preliminary Design Review.

(3) Post Preliminary Design Review delivery of system to the government for acceptance testing.

(4) From acceptance through pre-fielding.

(5) Post pre-fielding through operational deployment.

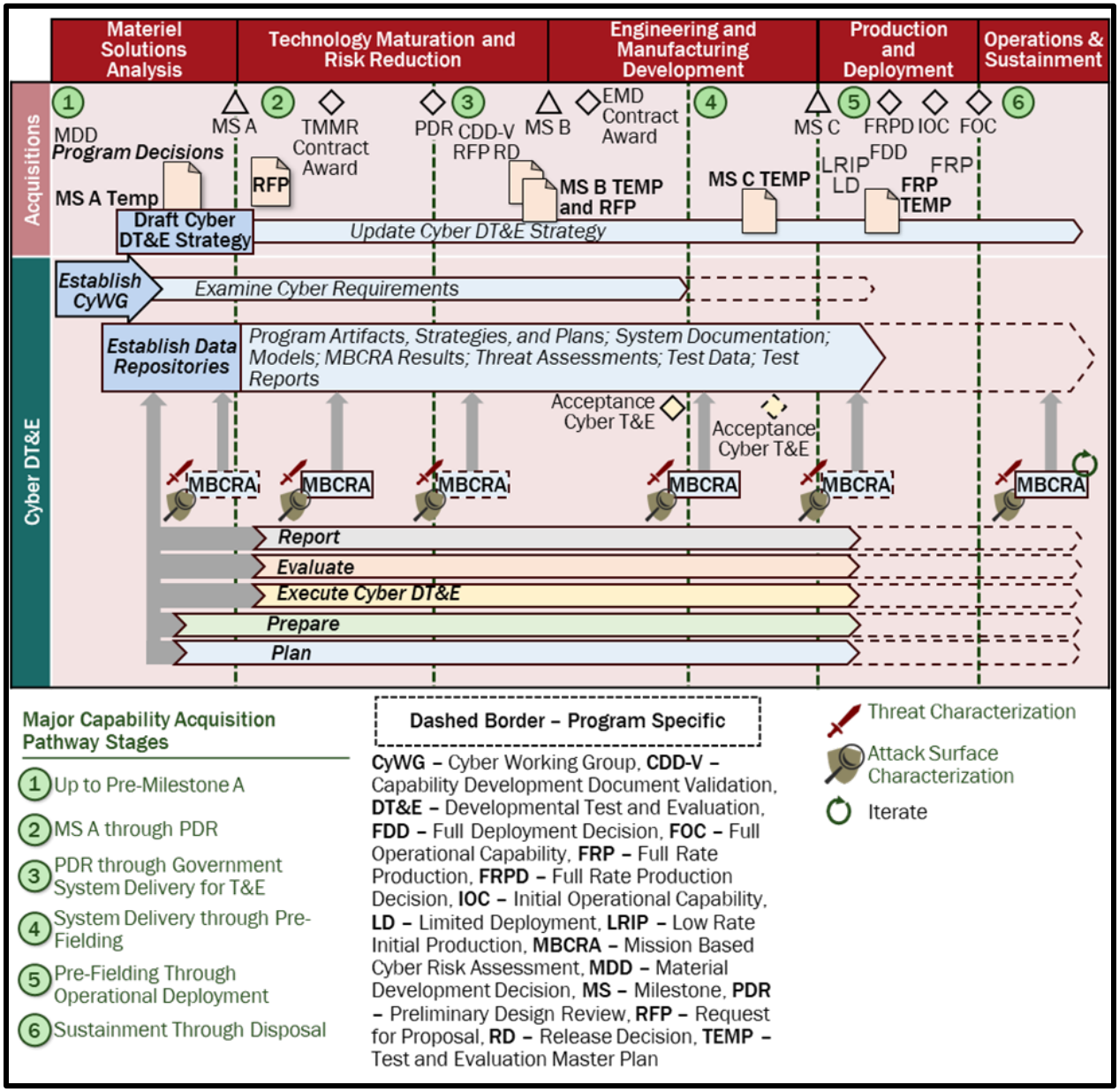
(6) Sustainment through disposal.

b. Figure 6 provides a sample of cyber DT&E activities for the MCA pathway schedule, based on Table 7.

Table 7. MCA Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3	4	5	6
Establish and charter the CyWG	●					
Examine and advise on cyber requirements	●	●	●	●	○	
Examine threat assessments and characterize attack surface	●	●	●	●	●	●
Support criticality and MRT-C analysis	●	↻	↻	↻	↻	○
Conduct or update MBCRA	○	●	○	●	○	↻
Develop or update cyber DT&E strategy	●	↻	↻	↻	↻	○
Determine test infrastructure, tools, and data requirements	●	↻	↻	↻	↻	○
Plan resources and schedule government cyber DT&E		●	↻	↻	↻	○
Include cyber DT&E requirements in each RFP and contract	●	●	●			
Review system developer (contractor) or government development and test environment, processes, and tools		●	↻	○	○	○
Analyze existing or known vulnerabilities		●	●	●	●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received		●	●	○	○	○
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing		●	●	●	●	●
Conduct test readiness reviews		●	●	●	●	●
Execute security verification throughout the system's life cycle		●	●	●	●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system		●	●	○	○	○
Execute planned government acceptance cyber T&E			●	○		
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events				●	●	○
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies		●	●	●	●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones required pursuant to DoDI 8510.01		●	●	●	●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●	●	●	●
Plan and update sustainment cyber DT&E activities and frequency			●	↻	↻	○

Figure 7. Sample Cyber DT&E Activities for the MCA Pathway



5.5. SOFTWARE ACQUISITION PATHWAY.

a. Table 8 outlines program activities in three stages for the software acquisition pathway:

(1) Planning.

(2) Execution Pre-Minimum Viable Capability Release.

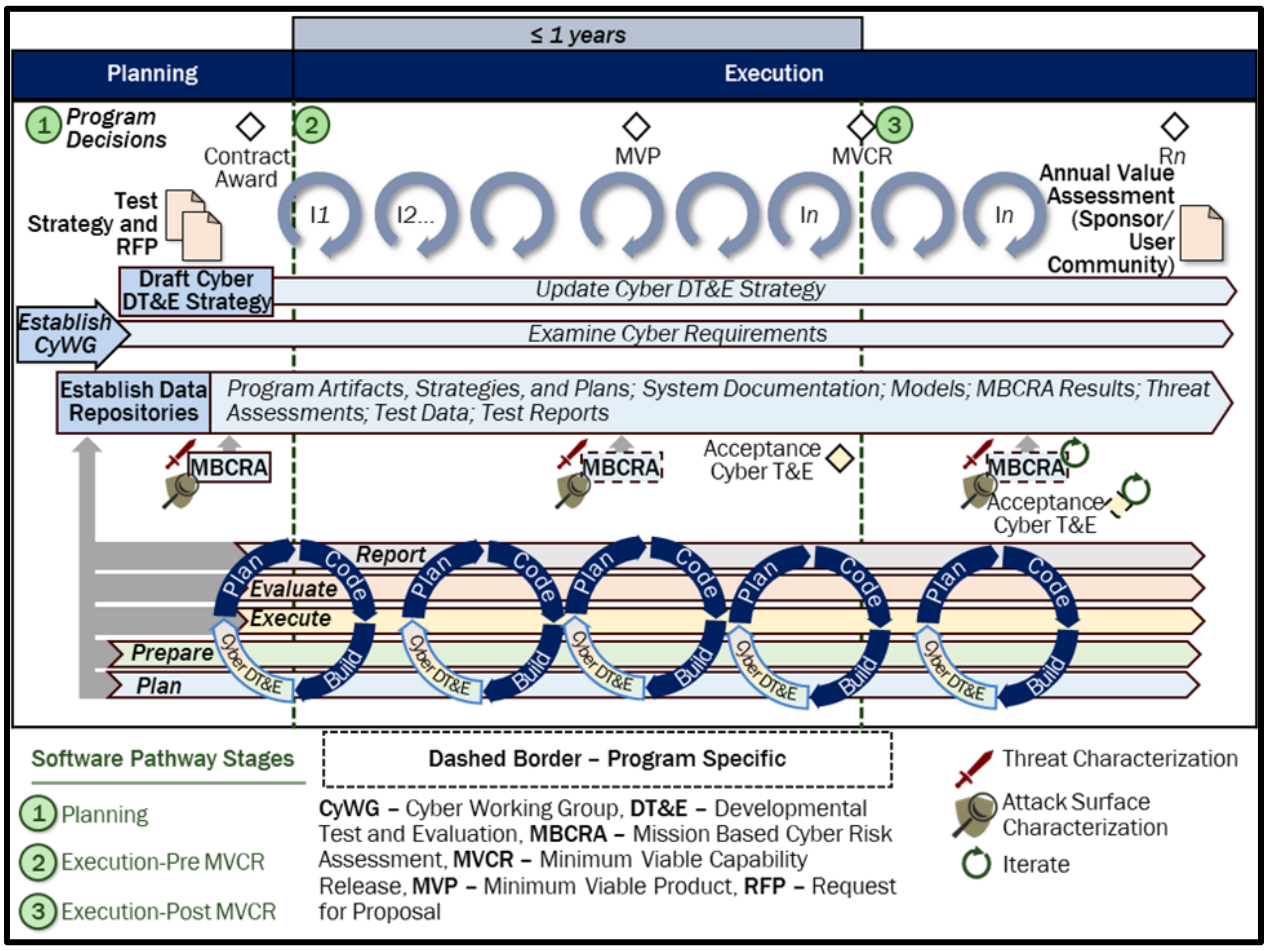
(3) Execution Post-Minimum Viable Capability Release. In Stage 3, the program sets the pace for required activities.

b. Figure 7 provides a sample of cyber DT&E activities for the software acquisition pathway schedule, based on Table 8.

Table 8. Software Acquisition Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3
Establish and charter the CyWG	●		
Examine and advise on cyber requirements	●	●	●
Examine threat assessments and characterize attack surface	●	●	●
Support criticality and MRT-C analysis	●	↻	↻
Conduct or update MBCRA	●	○	○
Develop or update cyber DT&E strategy	●	↻	↻
Determine test infrastructure, tools, and data requirements	●	↻	↻
Plan resources and schedule government cyber DT&E	●	↻	↻
Include cyber DT&E requirements in each RFP and contract	●	○	○
Review system developer (contractor) or government development and test environment, processes, and tools	●	↻	↻
Analyze existing or known vulnerabilities		●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received		●	●
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing		●	●
Conduct test readiness reviews		●	●
Execute security verification throughout the system's life cycle		●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system		●	●
Execute planned government acceptance cyber T&E		●	○
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events		●	●
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies		●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01		●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●
Plan and update sustainment cyber DT&E activities and frequency	●	↻	↻

Figure 8. Sample Cyber DT&E Activities for the Software Acquisition Pathway



5.6. DEFENSE BUSINESS SYSTEM (DBS) ACQUISITION PATHWAY.

a. Table 9 outlines program activities in five stages for the DBS pathway:

(1) Capability Need Identification.

(2) Solution Analysis.

(3) Functional Requirements and Acquisition Planning.

(4) Acquisition Testing and Deployment.

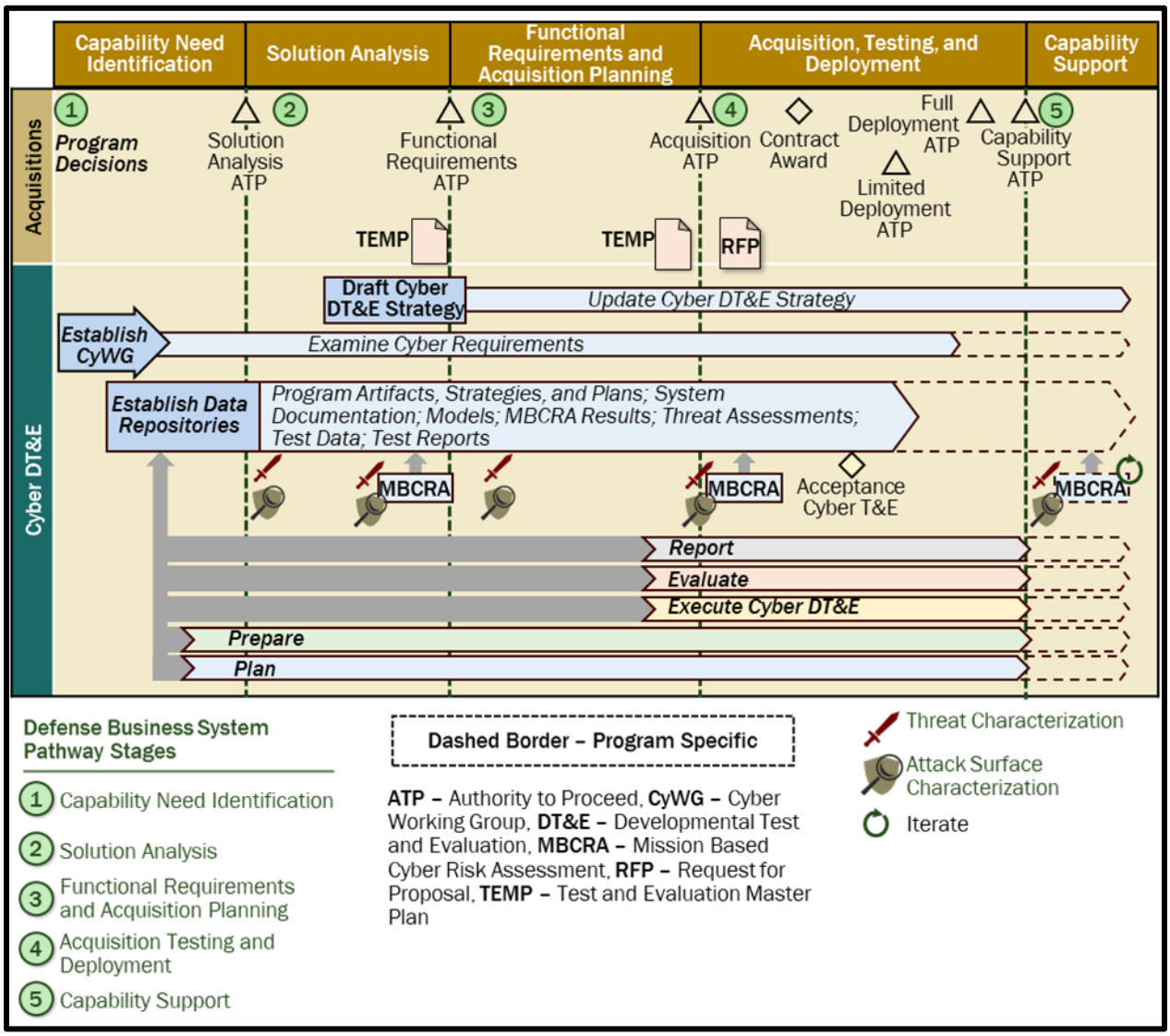
(5) Capability Support.

b. Figure 8 provides a sample of cyber DT&E activities for the DBS pathway schedule, based on Table 9.

Table 9. DBS Acquisition Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3	4	5
Establish and charter the CyWG	●				
Examine and advise on cyber requirements	●	●	●	●	○
Examine threat assessments and characterize attack surface	●	●	●	●	●
Support criticality and MRT-C analysis	●	↻	↻	↻	○
Conduct or update MBCRA		●		●	○
Develop or update cyber DT&E strategy			●	↻	↻
Determine test infrastructure, tools, and data requirements			●	↻	↻
Plan resources and schedule government cyber DT&E			●	↻	↻
Include cyber DT&E requirements in each RFP and contract		●	↻	○	○
Review system developer (contractor) or government development and test environment, processes, and tools				●	↻
Analyze existing or known vulnerabilities		●	●	●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received				●	↻
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing				●	●
Conduct test readiness reviews				●	●
Execute security verification throughout the system's life cycle			●	●	●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system				○	
Execute planned government acceptance cyber T&E				●	
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events				●	○
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies				●	●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01				●	●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●	●	●
Plan and update sustainment cyber DT&E activities and frequency			●	↻	↻

Figure 9. Sample Cyber DT&E Activities for the DBS Acquisition Pathway



5.7. ACQUISITION OF SERVICES PATHWAY.

a. Due to cyber risks in commercial information technology acquired services, the program will conduct cyber DT&E to inform the project and assess mission risks. Table 10 outlines program activities in three stages for the acquisition of services pathway:

(1) Plan.

(2) Develop.

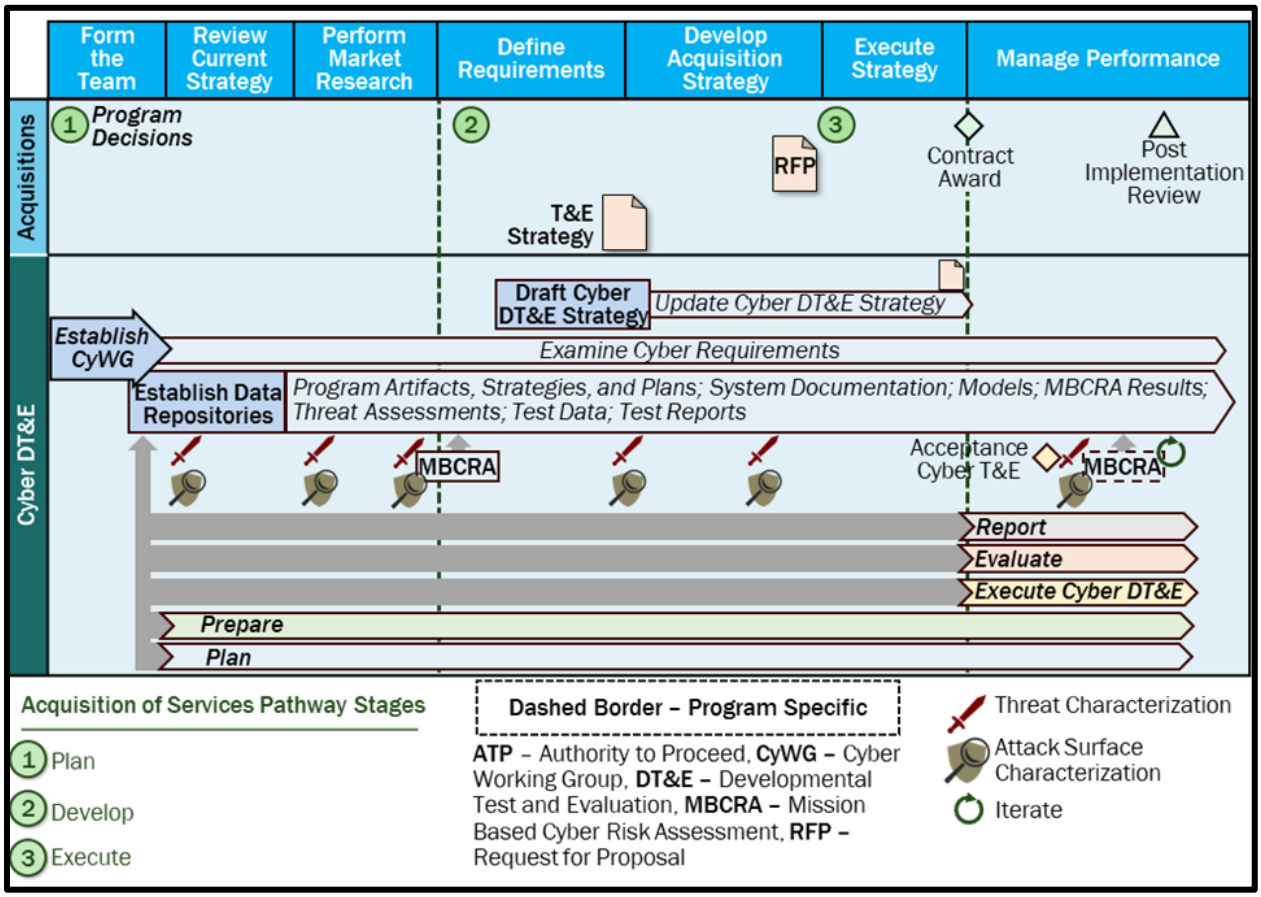
(3) Execute.

b. Figure 9 provides a sample of cyber DT&E activities for the acquisition of services pathway schedule, based on Table 10.

Table 10. Acquisition of Services Pathway Program Activities

● Required, ○ Recommended or Program-Specific, ↻ Required Update	1	2	3
Establish and charter the CyWG	●		
Examine and advise on cyber requirements	●	●	●
Examine threat assessments and characterize attack surface	●	●	●
Support criticality and MRT-C analysis	●	●	●
Conduct or update MBCRA		●	○
Develop or update cyber DT&E strategy		●	↻
Determine test infrastructure, tools, and data requirements		●	↻
Plan resources and schedule government cyber DT&E		●	↻
Include cyber DT&E requirements in each RFP and contract		●	↻
Review system developer (contractor) or government development and test environment, processes, and tools			●
Analyze existing or known vulnerabilities		●	●
Review system developer (contractor) cyber DT&E strategy and all test plans as received			●
Leverage all available and relevant test data for test planning and ensure all test data is available for subsequent testing			●
Conduct test readiness reviews			●
Execute security verification throughout the system's life cycle			●
Execute planned system developer (contractor) or integrated government-contractor cyber developmental testing of subcomponent through prototype or developed system			●
Execute planned government acceptance cyber T&E			●
Execute planned government cyber DT&E or integrated cyber developmental and operational tests with independent evaluations, and regression test events			●
Review cyber test results, as received, plans for remediation and regression testing, and recommend mitigation strategies			●
Integrate cyber test results with the security assessment report, risk assessment report, and plan of action and milestones pursuant to DoDI 8510.01			●
Report on cyber DT&E activities and deficiencies, make documentation, data, and reports available to authorized users	●	●	●
Plan and update sustainment cyber DT&E activities and frequency		●	↻

Figure 10. Sample Cyber DT&E Activities for the Acquisition of Services Pathway



GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AI	artificial intelligence
ATO	authority to operate
BOM	bill of materials
CDAO	Chief Digital and Artificial Intelligence Officer
CDT	chief developmental tester
CyWG	cyber working group
DBS	defense business system
DoDD	DoD directive
DoDI	DoD instruction
DoW	Department of War
DoW CIO	DoW Chief Information Officer
DT&E	developmental test and evaluation
EMSO	electromagnetic spectrum operations
FSSL	full spectrum survivability and lethality
IATT	interim authorization to test
IDSK	integrated decision support key
IP	Internet Protocol
ITT	integrated test team
MBCRA	mission-based cyber risk assessment
MCA	major capability assessment
MRT-C	mission-relevant terrain in cyberspace
M&S	modeling and simulation
MTA	middle tier of acquisition
OSW	Office of the Secretary of War
OT&E	operational test and evaluation
PL	public law
PPP	program protection plan
RFP	request for proposal
RMF	risk management framework

ACRONYM	MEANING
S&T	science and technology
T&E	test and evaluation
TEMP	test and evaluation master plan
TTPs	tactics, techniques, and procedures
UCA	urgent capability acquisition
U.S.C.	United States Code
USW(A&S)	Under Secretary of War for Acquisition and Sustainment
USW(I&S)	Under Secretary of War for Intelligence and Security
USW(R&E)	Under Secretary of War for Research and Engineering
WIPT	working-level integrated product team

G.2. DEFINITIONS.

A complete glossary of acquisition terms is maintained on the Defense Acquisition University website. The Defense Acquisition University Glossary can be found at https://www.dau.edu/tools/dau-glossary. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
acquisition category ID	Defined in the Defense Acquisition University Glossary.
anomaly	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/anomaly.
attack path	A visual representation of an attack through the specific MRT-C through which an adversary would progress from the attack surface.
attack path analysis	An assessment of attack path vulnerabilities, and the sequence of steps an attacker might take to impact the mission or safety critical functions.
attack surface	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/attack_surface.
attack surface diagram	A diagram that identifies and relates system missions, mission essential functions, components, communication paths, insider areas of concern, attack paths, designed-in dependencies, and mission-essential nodes or exposures.

TERM	DEFINITION
BOM	A formal record containing the details and supply chain relationships of various components used in building a system's firmware, hardware, and software.
contested cyber environment	An environment in which cyberspace threat actors, competing entities, and entities with similar resource needs contend for control or use of cyber resources.
contract data requirements list	Defined in the Defense Acquisition University Glossary.
critical component	Defined in the Defense Acquisition University Glossary.
criticality analysis	Defined in DoDI 5200.44.
cyber defender	Anyone who actively participates in identifying, protecting, detecting, responding to, and recovering from cyberspace attacks on a system (e.g., operator, cybersecurity service provider, maintainer, or system administrator).
cyber DT&E	The subset of T&E activities, tools, data, and artifacts used to create independently verifiable and substantiated knowledge to quantify and characterize the cyber resilience of a system, subsystem, component, and software or to create independently verifiable and substantiated information to quantify and characterize cyber-related utility and risks of new technologies under development, such as those in the S&T development phase.
cyber physical system	A system integrating computation with physical processes whose behavior is defined by both the computational (digital and other forms) and the physical parts of the system.
cyber range	Defined in DoDD 5101.19E.
cyber resilience	The cyber component of operational resilience.
cybersecurity	Defined in the Committee on National Security Systems Instruction 4009.
cyberspace	Defined in the DoD Dictionary of Military and Associated Terms.
cyberspace attack	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
cyberspace event	An occurrence or condition, including system faults, not yet assessed, that may affect the system's behavior and outcomes resulting in harm, destruction, or loss of ability to perform required capability during operation.
cyberspace threat	Any intended or unintended circumstance or event that may adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via any combination of unauthorized access, destruction, disclosure, modification of information, denial of service.
data item description	Defined in the Defense Acquisition University Glossary.
data poisoning	The deliberate and malicious contamination of data to compromise the performance of AI and machine learning systems.
decision authority	Defined in the Defense Acquisition University Glossary.
Defense Acquisition System	Defined in the Defense Acquisition University Glossary.
deficiency	Any condition that limits or prevents the use of materiel for the purpose intended or required, although the materiel may meet all other specifications or contractual requirements. These conditions cannot be corrected except through a design or specification change.
derived cyber performance requirements	Cyber performance requirements created from higher-level requirements after considering constraints, issues implied but not explicitly stated in the requirements baseline, factors introduced by the selected architecture, and design.
digital twin	Defined in DoDI 5000.97.
hardware-in-the-loop facility	Hardware-in-the-loop facility connects real-world equipment to a real-time simulator to enable testing to evaluate the performance, functionality, and safety of controllers and protection systems.
IATT	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/interim_authorization_to_test.
IDSK	Defined in DoDI 5000.89.

TERM	DEFINITION
incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
integrated testing	Defined in DoDI 5000.89.
Joint Deficiency Reporting System	A cross-service web enabled automated tracking system designed to initiate, process, and track deficiency reports from the warfighter through the investigation process (located at https://jdrs.mil/). Joint Deficiency Reporting System-Classified is also available, as required.
logistics demonstration	Defined in the Defense Acquisition University Glossary.
MBCRA	The analytical process of identifying, estimating, assessing, and prioritizing risks based on impacts on DoW operational missions resulting from cyber effects on the system(s) being employed. A cyber table top is an example of a methodology used to conduct an MBCRA.
milestone decision authority	Defined in the Defense Acquisition University Glossary.
military handbook	A document that establishes uniform engineering and technical requirements for military-unique or substantially modified commercial processes, procedures, practices, and methods.
mission critical function	Any function that, if compromised, would degrade the system effectiveness in achieving the core mission for which it was designed.
mitigation	Act of reducing risk by taking some other action generally outside the influenced system's domain, which cannot be remediated.
MRT-C	All devices, internal links, external links, operating systems, services, applications, ports, protocols, hardware, software on servers, and other technical aspects of a system required for the function of a critical asset; may exist external to the DoW cyberspace.
National Vulnerability Database	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/nvd.

TERM	DEFINITION
operational resilience	Defined in DoDI 8500.01.
penetration testing	A cyber test involving efforts to circumvent or defeat the security features and simulate cyberspace attacks against the system under test to verify that new and existing software, hardware, firmware, interfaces, communications, data, networks, and systems are not vulnerable to exploitation.
purple team testing	A cyber test that uses the knowledge and tools of both the adversarial and cooperative test teams to identify weaknesses in security controls, processes, and procedures.
remediation	Actions taken to eliminate an identified risk.
responsible cyber DT&E team	A multidisciplinary group of qualified personnel, which may be from the government, a system, subsystem or component developer, a third-party, etc., or a combination of such organizations, tasked with preparing, executing, evaluating, and reporting on cyber developmental testing activities to assess the cybersecurity and cyber resilience of DoW systems.
RMF	Defined in the Defense Acquisition University Glossary.
safety critical function	A function whose failure to operate or incorrect operation will directly result in a mishap of either catastrophic or critical severity.
security verification	A process using automated scripts and other tools to identify known vulnerabilities in the system under test. Examples include scanning for security technical implementation guidance configuration for network devices, software, databases, and operating systems, and conducting software assurance processes (e.g., fuzzing) to gain confidence and trustworthiness in vulnerability discovery.
supply chain	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/supply_chain.
supply chain risk	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/supply_chain_risk.
system fault	An abnormal condition or defect that disrupts a system's proper functioning.

TERM	DEFINITION
system under test	The subcomponent(s), component(s), subsystem(s), system(s), or system-of-systems which are the focus of the test, including representative users, maintenance devices, and other periphery equipment.
systems security working group	A cross-functional team that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security.
T&E	Defined in the Defense Acquisition University Glossary.
TTPs	The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures give an even lower-level, highly detailed description in the context of a technique.
vulnerability	A verified weakness in a system, embedded sub-system, platform, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system – resulting in a security incident or a violation of the system's security policy (e.g., a known software vulnerability that is actively being exploited).
vulnerability assessment	A cyber test providing a systematic examination of a system using all available documentation (e.g., system design, source code, manuals) to identify deficiencies or vulnerabilities, and measure the adequacy of prevent, detect, and contain capabilities when attempting to circumvent or defeat defensive capabilities.
weakness	Defined in the National Institute of Standards and Technology Glossary at https://csrc.nist.gov/glossary/term/weakness.

TERM	DEFINITION
white card	Skipping parts of the cyberspace attack methodology, (e.g., gaining initial access), to focus on specific aspects of the attack methodology in which the stakeholders are most interested. May be used if a system is too fragile or operationally critical for the cyber test team to pursue exploitation, or when the cyber test team is unable to penetrate the system, but there is still a desire to evaluate the system's ability to react to a penetration while collecting tactical or operational risk to the mission.
zero trust	Defined in the Defense Acquisition University Glossary.

REFERENCES

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems Glossary," March 2, 2022

Defense Federal Acquisition Regulation Supplement, current edition

DoD Cybersecurity Reference Architecture, current edition

DoD Cyber Table Top Guide, current edition

DoD Data Analytics, and Artificial Intelligence Adoption Strategy, November 2023

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

DoD Directive 5101.19E, "DoD Executive Agents for the Cyber Test and Cyber Training Ranges," August 24, 2018

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

DoD Directive 5205.07, "Special Access Program Policy," September 12, 2024

DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020

DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018, as amended

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

DoD Instruction 5000.61, "DoD Modeling and Simulation Verification, Validation, and Accreditation," September 17, 2024

DoD Instruction 5000.79, "Defense-Wide Sharing and Use of Supplier and Product Performance Information (PI)," October 15, 2019

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

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

DoD Instruction 5000.97, "Digital Engineering," December 21, 2023

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.44, "Protection of Mission and Critical Functions to Achieve Trusted Systems and Networks," February 16, 2024

DoD Instruction 8140.02, "Identification, Tracking, and Reporting of Cyberspace Workforce Requirements," December 21, 2021

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

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

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

DoD Instruction 8530.03, "Cyber Incident Response," August 9, 2023

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

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

DoD Responsible Artificial Intelligence Toolkit, November 2023

DoD Systems Engineering Plan Outline, current edition

DoD Zero Trust Reference Architecture, current edition

Federal Acquisition Regulation, current edition

Military Handbook MIL-HDBK-1553A, "Multiplex Applications Handbook," November 1, 1988

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

Public Law 115-91, Section 1640, "National Defense Authorization Act for Fiscal Year 2018," December 17, 2017

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

United States Code, Title 10