TEST AND EVALUATION ENTERPRISE GUIDEBOOK

August 2022

FOREWORD

The T&E Enterprise Guidebook further clarifies and details the procedures that should be implemented to meet the intent of the T&E policies outlined in DOD Instruction (DoDI) 5000.89. The T&E Enterprise Guidebook clarifies the T&E role and actions for five of the six acquisition pathways detailed in DoDI 5000.02: major acquisition capability, middle tier of acquisition, urgent capability acquisition, defense business systems, and software acquisition pathway. The role of T&E for the acquisition of services will be provided if the pathway is used in the future to deliver critical warfighting capabilities. Irrespective of the acquisition pathway, the T&E Enterprise Guidebook emphasizes the need for T&E professionals to do the following:

- Actively engage in the acquisition process at the onset of the acquisition program to inform the development of the requirements and acquisition contracts;

- Collaborate in the planning and execution of T&E events across the system lifecycle to provide data early and often in support of both developmental and operational test objectives and acquisition decisions while supporting timely assessments of progress and risk to technical and operational performance;

- Actively engage with program managers to establish and enable the use of data stores and knowledge management tools to successfully build the body of evidence needed to support more agile T&E; and

- Leverage digital engineering tools, rigorous verification and validation processes, and automation tools to expedite the T&E planning, data analysis, reporting, and management of identified design shortfalls and vulnerabilities.

We expect to update the T&E Enterprise Guidebook as new challenges arise and as new T&E tools and processes become available to support even more agile and robust T&E. This memorandum applies to all future updates to the T&E Enterprise Guidebook that will include an array of T&E Focus Area Chapters intended to provide additional guidance on unique topics such as cyber survivability, artificial intelligence-based systems, modeling and simulation, interoperability, and more.

Adequate and agile T&E is the cornerstone of delivering weapons that work, at the speed of operational relevance. For programs on the T&E Oversight List, we will consider adherence to the T&E Enterprise Guidebook in our review of the adequacy of T&E strategies and plans. Regardless of the oversight status, we strongly encourage all to adhere to the procedures outlined in this T&E Enterprise Guidebook.

Heidi Shyu
Under Secretary of Defense
for Research and Engineering

Nickolas H. Guertin
Director
Operational Test and Evaluation

Table of Contents

TEST AND EVALUATION CHAPTER 1: T&E OVERVIEW

Table of Contents

Test and Evaluation (T&E) Overview

1. Introduction

The Enterprise T&E Guidebook provides the DoD Acquisition and T&E communities with the requisite information to comply with the T&E Policy specified in DoDI 5000.89 and facilitate a robust and rigorous T&E program. In the event of conflict between this guidance and the policy, the reader should defer to policy documentation. The Enterprise T&E Guidebook consists of three parts:

- **T&E Overview.** Provides readers with foundational information about T&E applicable across the six pathways outlined in the DoD's Adaptive Acquisition Framework (Figure 1). In particular, the T&E Overview identifies types of T&E within the DoD; required T&E documentation; T&E roles, responsibilities, and authorities; the T&E Oversight List; and general information about managing a T&E program.
- **T&E Acquisition Pathway Guidance.** Provides readers with information about the T&E activities that defense acquisition programs should undertake for each acquisition pathway within the DoD's Adaptive Acquisition Framework: Major Capability Acquisition, Urgent Capability Acquisition, Middle Tier of Acquisition, Defense Business Systems, and Software Acquisition. The requirement for additional information about the Acquisition of Services pathway is under review.
- **Focus Areas.** Provide readers with information on critical assessment areas for T&E, such as cybersecurity, and enablers of T&E, such as T&E strategies. Focus area chapters will evolve and links will be provided as they are created.

Throughout the Enterprise T&E Guidebook, you will also encounter references to Companion Guides which provide detailed how-to information on particular T&E activities, methods, and documentation. Links will appear as companion guides become available, and additional companion guides will be developed as appropriate.

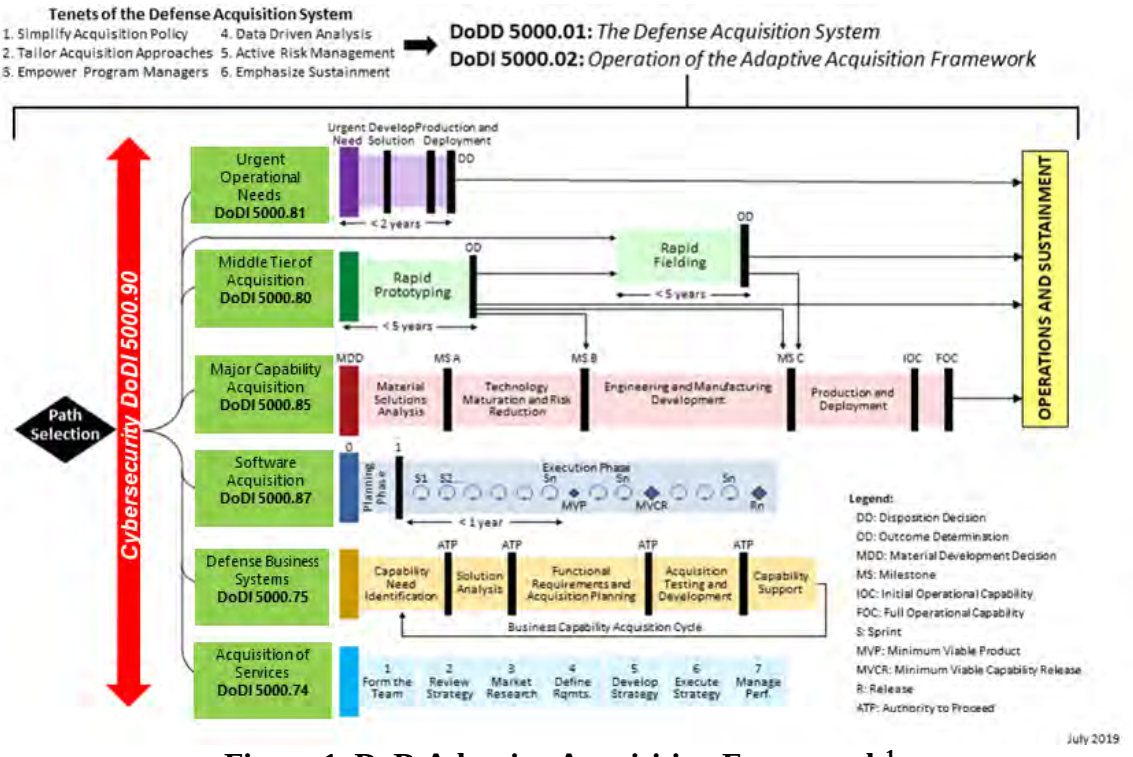


Figure 1. DoD Adaptive Acquisition Framework[1]

1.1 Purpose of T&E

T&E is critical to the acquisition process, as it provides the data required to demonstrate technical, functional, and warfighting capability, and affords the opportunity to identify and solve any system deficiencies prior to making a final acquisition or fielding decision. The effectiveness and efficiency of the T&E program is enhanced by two major factors: 1) an adequately planned and resourced T&E strategy and 2) access to contractor-generated data, tools, information, and expertise. Adequate T&E provides engineers and decision makers with knowledge to assist in managing programmatic risks, measuring technical progress, and characterizing operational effectiveness, suitability, survivability, and lethality as the program progresses through the acquisition process.

The Program Manager (PM) should involve the T&E organizations with the acquisition program from its inception and throughout its lifecycle to support the program decisions and delivery timeline. Contractor testing (CT), government developmental test and evaluation (DT&E), live fire test and evaluation (LFT&E), and operational test and evaluation (OT&E) should be integrated, streamlined, and automated to the maximum extent practicable to enable efficient use of test data and resources across the test program and evaluation of system operational effectiveness, suitability, survivability, and lethality to inform the decision authorities. Maximum sharing, reciprocity, availability, and reuse of test results and artifacts among testing and certification organizations are necessary for efficiency. Collaboration between all organizations should be considered to develop

[1] DoDI 5000.02

digital system models, simulations, and test environments for common use across the spectrum of system tests that may produce necessary data or information. The PM should capture results from all test events in a shared data repository, available for all parties to use for independent assessment:

- Government test teams should be involved from the inception of the program to ensure their T&E requirements are captured in acquisition contracts and that they have a process to generate the required data.
- Government test teams should strive to maintain a tempo that supports the required decisions using various tools (e.g., digital engineering, sequential testing, and automation).
- Government test teams should develop a robust T&E program to support decisions with end-to-end mission threads employing actual users.
- OT&E and LFT&E should concentrate on appropriately scoped, dedicated tests while integrating useable data and information from all sources to meet stakeholder needs, support operational evaluations, and inform decisions.
- The T&E Working Integrated Product Team (WIPT) may develop collaborative test data scoring boards to evaluate available test data for potential to meet any IOT&E and LFT&E requirements.

2. Types of Test & Evaluation

Each type of T&E exists to enable the DoD to acquire systems that support warfighters in accomplishing their mission. Collaborative planning and execution of test phases and events can provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders. This approach does not support the replacement of dedicated DT&E, OT&E, or LFT&E, but may affect the scope of individual test events if stakeholders can pull data from prior events to support their evaluations. Incorporating operational realism early in the test program improves the probability of identifying and correcting problems early, rather than later in development when redesigns are more expensive and correcting the problem may prove infeasible.

Before the start of testing for any acquisition path, the T&E WIPT will develop a T&E Strategy[2] to document DT&E, OT&E, and LFT&E requirements; the rationale for those data requirements (e.g., Joint Capabilities Integration and Development System and a Concept of Operations (CONOPS)); and resources required, to be approved by the DOT&E and USD(R&E), or their designee, as appropriate.[3]

2.1 Developmental Test & Evaluation

DT&E is the disciplined process of generating substantiated knowledge on the capabilities and limitations of systems, subsystems, components, software, and materiel.

---

[2] Different naming conventions for the T&E planning document are common and acceptable (e.g. Simplified Acquisition Master Plan (SAMP), Test and Evaluation Master Plan (TEMP), test strategy, T&E Strategy). This document will refer to any of these as the T&E Strategy.

[3] DoDI 5000.89, pg. 10

This knowledge is used to inform decision makers on risks in acquisition, programmatic, technical, and operational decisions throughout the acquisition life cycle. DT&E assesses the maturity of technologies, system design, readiness for production, acceptance of government ownership of systems, and readiness to participate in operational T&E, and sustainment.

Both test and evaluation are necessary to gain value from a DT&E effort. In the context of DT&E, an entity can be a technology, process, materiel, software module, component, subsystem, system, and system of systems. Identified conditions refer to test conditions that are controlled, uncontrolled, measured, or not measured. Developmental evaluations are accomplished using criteria derived from various sources, the most common of which are the mission sets from the Concept of Operations/Operational Mode Summary/Mission Profile (CONOPS/OMS/MP), the capability gaps, user requirements specified in the capabilities documents (Initial Capabilities Document (ICD), the Capability Development Document (CDD), Critical Operational Issues (COIs), Critical Operational Issues and Criteria (COIC)), the design measures contained in the technical requirements documents (TRD), and contractual performance specifications. The data collected during one test may result in multiple developmental evaluations being accomplished.

DT&E activities should commence during the development of requirements to ensure key technical requirements are measurable, testable, and achievable, and provide feedback that the system engineering process is performing adequately. In particular, the DT&E program should:

- Verify the achievement of critical technical parameters and key performance parameters
- Assess system specification compliance and the system's ability to achieve the thresholds prescribed in the capabilities documents
- Provide data to the PM to enable root cause determination of failures arising from tests, and identify corrective actions
- Provide information for cost, performance, and schedule tradeoffs
- Report on the program's progress to plan for reliability growth, and assess reliability and maintainability performance for use during key program decisions
- Identify system capabilities, limitations, and deficiencies
- Assess system safety and compatibility with legacy systems
- Stress the system within the intended operationally relevant mission environment to assess readiness for OT
- Support all appropriate certification processes
- Document achievement of contractual technical performance, and verify incremental improvements and system corrective actions
- Assess entry criteria for IOT&E and FOT&E
- Provide DT&E data to validate parameters in modeling and simulation (M&S)
- Assess the maturity of the chosen integrated technologies

- Identify cyber vulnerabilities within custom and commodity hardware and software on components, subsystems, and systems so the Program Office can mitigate them early in the program's lifecycle
- Support cybersecurity assessments and authorization, including Risk Management Framework (RMF) security controls

b. Evaluation of Developmental Test Adequacy

DT&E provides feedback to the PM's and decision makers to inform decision-making throughout the acquisition cycle. The PM uses the T&E Strategy as the primary planning and management tool for the integrated test program. The documentation should describe a logical DT&E strategy, including: 1) decisions to be informed by the DT&E information, 2) evaluations to inform those decisions, 3) test and M&S events to be conducted to generate the data for the evaluation, and 4) resources to be used and schedules to be followed to execute T&E events. A comprehensive DT&E program generates the key data used to evaluate technologies, components, sub-systems, interoperability, cybersecurity, and reliability capabilities. The T&E Strategy includes an Integrated Decision Support Key (IDSK) and evaluation framework (if necessary) that shows the correlation/mapping between decisions, capabilities to be evaluated, measures to be used to quantify the capabilities, and test and M&S events.

2.2 Operational Test & Evaluation

OT&E supports the evaluation of the operational performance of units equipped with systems operated under realistic operational conditions in an operationally representative threat environment (Initial Operational Capability, plus ten years), including joint combat operations and system of systems concept of employment. Operational testing provides data required to enable credible evaluation of operational effectiveness, suitability, and survivability (10 U.S.C. §§ 4171 and 4172; DoDI 5000.89).

To this end, in 2019, the operational test community created, and DOT&E endorsed, a set of six core test principles intended to deliver more lethal and more resilient capabilities at the "speed of relevance." The six principles are: Early OT Involvement, Tailor to the Situation, Continuous and Cumulative Feedback, Streamline Processes and Products, Integrated and Combined Collection/Test, and Adaptive.

Early OT Involvement: The intent of this principle is for the OT teams to be engaged with a program from its very inception. The earlier an OT team's involvement, the greater its influence on requirements definition, budgeting, contracting, and engineering to ensure the entire test community is part of a system's development. By applying an operational perspective very early in a program, we can reduce changes later in the acquisition lifecycle and, in turn, reduce overall program cost.

Early involvement is more than "observation" from an oversight prospective or "being seated at the table" as a symbol of collaboration; it means truly being part of the team to ensure relevant and credible information is provided to the decision makers when they

need it. Early OTA involvement means shaping each test event to simultaneously meet Contractor Test (CT), Developmental Test (DT), and OT objectives. In other words, to the maximum extent possible, design test events in an environment that can collect data once to answer the respective test objectives.

Tailor to the Situation: The intent of this principle is to provide test teams the flexibility to adjust their tests as needed in order to field capabilities as rapidly as possible. Given that many programs today are rapid in nature and the acquisition community works hard to speed product delivery by exploring streamlined approaches and more agile techniques to procure products, our OT teams will need to adjust our methods to meet the unique needs of every program. We want each of our teams to know they have the flexibility to tailor their test planning, execution, and reporting as needed to field capability as rapidly as possible.

As each test team builds a test design for their program, they should determine and align the overarching purpose of the test with the warfighter ("characterize" versus "demonstrate"). What decision is being supported? What information is needed to support that decision? It is essential, in the spirit of the OTAs providing warfighting capability, that the warfighter has direct input and rationale as to why OT is being conducted. This information will be critical as we march toward the "speed of relevance."

Continuous and Cumulative Feedback: The intent of this principle is to ensure that OT provides timely feedback regarding the problems it discovers throughout the life of a program, especially in the earlier stages. The current acquisition timeline calls for OT reports at specific milestones in the process. With today's fast-paced acquisitions, these reports may be irrelevant even before publication. In order to provide relevant information, we will provide "Continuous and Cumulative Feedback" to the Program Office and all stakeholders regarding our findings. Depending on the nature of the program, we may still provide reports at specified milestones, but these reports will be a cumulative document containing all the OT feedback leading up to that particular milestone or decision point. We want the developer and the Program Manager to know test results almost as fast as the OT teams. This approach changes the paradigm from OT being a "final exam" for a Program Manager to OT being a partner in the system development, and yet still delivering combat capability through timely, independent assessments.

Streamline Processes and Products: Closely aligned with the principle of "Tailor to the Situation," the intent of this principle is to remove the bureaucratic constraints of the current acquisition processes. As a new program comes online, test teams should have the flexibility to modify existing procedures. To enable fielding at the "speed of relevance," the test team must have the ability to streamline test processes and products to best meet the needs of their program. Along these lines, and tied to the previous principle, we want the teams to be able to create new products and processes, as needed, as they plan, execute, and report on their systems.

Integrated and Combined Collection/Test: Closely coupled with "Early OT Involvement," the goal of this principle is to merge the primary test stakeholders (the

contractor/developer testers CT, DT, and OT) into one unified test team. As the program progresses through its acquisition lifecycle, we will no longer conduct sequential testing but pursue synchronized collection and data sharing among all three test communities. We should remove the artificial CT, DT, and OT barriers and think in terms of utilizing all test events at any point in the program to achieve CT, DT, and OT objectives in a collaborative fashion to the maximum extent possible. This "One Team" approach enhances communication across the entire program and encourages earlier and faster testing.

Adaptive: With today's rapidly evolving technologies, the OTAs must be able to adapt to whatever program is presented to them. With the push within DoD for prototyping and its associated rapid fielding, the OTAs must not be encumbered by existing bureaucratic processes, but must be allowed the freedom to change as the test proceeds in order to take advantage of learning during the test process. They should not be constrained by a "checklist mentality" or rigid test designs that exceed the scope of the specific and evolving warfighter concerns.

Application of these core principles are essential to enabling our warfighters with equipment that works at the right time. The entirety of the T&E community alignment with these principles will facilitate early discovery and correction of deficiencies and collapse the artificial barriers between developmental and operational testing.

OT&E is conducted on all programs to support the development and fielding decisions. Following initial fielding, any capability upgrades that could materially change system performance will have to be tested to ensure no degradation in operational performance as a result of such changes, and to assess the extent of any improvements to performance as a result of those changes. Programs on T&E oversight may not conduct OT until the DOT&E approves the adequacy of plans in writing.

For programs under T&E oversight, the DOT&E may provide the Milestone Decision Authority (MDA) with a report summarizing the assessment of the test adequacy and operational performance findings in support of the milestone decisions. For programs on T&E oversight, DOT&E must submit a report to the Secretary of Defense and the congressional defense committees before programs are permitted to proceed beyond low-rate initial production (BLRIP), which will state the Director's opinion as to whether T&E was adequate and evaluate whether a unit equipped with the system was operationally effective, suitable, and survivable for combat. The Director may also provide additional information on the operational capabilities of the items or components as appropriate (10 U.S.C. §§ 4171 and 4172.).

2.3 Types of Operational Events

Operational events may be categorized into five types. Test plan approval for each test type varies and may be tailored as appropriate.

Operational demonstrations may be conducted by the material developer, PM, or operational test agency (OTA) with representative warfighters and missions to improve

system design, and should incorporate all aspects of system performance, including survivability and lethality, if deemed critical to mission effectiveness or force protection. The purpose of an ops demo is to assess the technical maturity and interoperability of the system, as well as characterize the system's progress in a threat-realistic operational environment. Data from such events may inform program transition decisions (e.g., exit from rapid prototyping) and subsequent OT events.

Early Operational Assessments (EOA) may be conducted to provide a means to evaluate a program's progress early in the process toward developing an operationally effective, suitable, and survivable system. EOAs are typically an analysis, based on a review of current program plans and documentation, as well as data from early developmental testing, technology assessments, M&S, and program reviews, to include the preliminary design review. EOAs enable the OTA to provide early input on key operational strengths and risks inherent to the design that, if not corrected, could have a detrimental effect on the determination of operational effectiveness, suitability, and survivability. EOAs examine the links and consistency between the CONOPS, requirements, and technology limitations to provide recommendations to the program and the requirements authority.

Operational Assessments (OA) should be conducted with operational realism to the maximum extent possible with representative units, missions, and environments and provide data to evaluate system performance. OAs often serve as risk reduction events to minimize the risk of finding major issues during IOT&E. An OA or a series of OAs may be conducted with pre-production systems and may not test the system in all missions and operational environments, or against all threats. Data from OAs may be analyzed and reported as an interim assessment of the status of the system's capability and limitations and any risks in meeting operational effectiveness, suitability, and/or survivability. In the event that an operational assessment is supporting a fielding or deployment decision, plans should detail system configuration, capabilities, users, missions, environment, and the data needed to demonstrate the required capabilities. In these cases, if the program is on T&E oversight, an early fielding report will document whether the system is operationally effective, suitable, and/or survivable in accordance with 10 U.S.C. §§ 4171 and 4172 .

Initial Operational Test and Evaluation (IOT&E) is required in Title 10 U.S.C. §§ 4171 for major defense acquisition systems to proceed to full rate production. IOT&E will use production or production-representative test articles in a dedicated field test conducted under realistic combat conditions to determine operational effectiveness, suitability, and survivability. Realistic combat conditions should include all relevant threats where possible, including, but not limited to: cyber, electromagnetic spectrum operations (EMSO), kinetic, directed energy, and chemical biological radiological nuclear (CBRN).

Follow-on Operational Test and Evaluation (FOT&E) may be necessary after IOT&E to evaluate system modifications or verify that identified deficiencies have been corrected. The scope of FOT&E should be tailored as appropriate. Data gathered during

FOT&E should ensure that the system retains its operational effectiveness, suitability and survivability, in a new or emerging operational environment or in a new mission.

2.4 Operational Test Readiness Review (OTRR)

OTRRs occur prior to an operational event (e.g., IOT&E, OA, FOT&E), and address and verify system reliability, maintainability, and supportability performance, as well as determine if the hazards and Environmental, Safety, Occupational, and Health (ESOH) and Software System Safety are manageable within the planned testing operations. The OTRR determines if changes are required in planning, resources, or testing necessary to proceed with OT&E. OTRRs may be conducted in multiple steps to ensure that the production configuration of the system (usually the LRIP system) can proceed to OT&E.

Programs on the T&E Oversight List are required by DoD policy to establish a Service process for determining and certifying a program's readiness for IOT&E by the Service or the Component Acquisition Executive. The OTRR is complete when the Service or the Component Acquisition Executive evaluates and determines material system readiness for IOT&E. The OTRR may be conducted by the PM or operational test agency (OTA), depending on Service policy.

2.5 Live Fire Test and Evaluation (LFT&E)

Live fire testing informs the degree to which a system, operating in a realistic threat environment, can avoid, withstand, or recover from threats it is likely to encounter in combat (survivability) or the ability of a weapon or weapon system to kill expected threats and targets in an operationally realistic environment (lethality). As with OT&E, "operationally representative" covers the period of IOC, plus ten years. The requirements to conduct LFT&E are contained in 10 U.S.C. §§ 4172. Survivability includes all classes of threats able to harm, deter, or destroy the system, including kinetic and non-kinetic threats.

LFT&E is not limited to testing system specifications and will test against threats likely to be encountered in combat or appropriate targets configured for combat. For survivability, the primary emphasis is on testing system vulnerability to kinetic attack with respect to user casualties while also considering susceptibility to attack, including the effect of those vulnerabilities on residual mission capability and recoverability from attack. Testing must include firing threats at the system as it is configured for combat, including all the dangerous materials (including flammables and explosives), and all critical subsystems present and operating that could make a difference in determining the test outcome. Crew and user casualties should include specific details on the type and severity of injury, as well as the potential operational impact of such casualties on the ability of the platform to accomplish its mission after a threat engagement, when appropriate. Personnel survivability must also be addressed even in cases where the platform cannot survive. For example, in cases of crash and egress. While user casualties

are a primary emphasis, uncrewed systems and weapons may also be subject to LFT&E to evaluate system survivability and effectiveness.

For lethality, the primary emphasis is on the evaluation of lethal effects of the weapon (munition or missile) on appropriate targets configured for combat. In testing of production-representative systems, the target should be representative of the class of systems the weapon is designed to defeat and demonstrate the lethality effects the weapon is designed to produce.

Survivability and lethality plans will be included in the T&E Strategy. Survivability and lethality testing starts early in a program's life cycle, allowing time to correct any design deficiency and vulnerabilities demonstrated by such testing. At the conclusion of LFT&E, the DOT&E shall submit a report on the adequacy of LFT&E testing and the survivability and lethality performance of the system/weapon to the congressional defense committees.

2.5.1.1 FUSL Waiver Process

In accordance with 10 U.S.C. §§ 4172(c), an LFT&E program must perform Full-Up System-Level (FUSL) testing. Although there is no waiver from LFT&E, the law contains provisions for a waiver from the requirements for FUSL testing. The Program Executive Officer will provide a memorandum to the Service or the Component Acquisition Executive asserting that the survivability or lethality tests required by 10 U.S.C. §§ 4172 are unreasonably expensive and impractical. The Service or the Component Acquisition Executive will provide a similar memorandum to USD(A&S) as the Defense Acquisition Executive requesting a waiver from the requirement of FUSL testing on that basis. The waiver must be approved by USD(A&S) as the DAE, even in cases where acquisition authority has been delegated to the Service.

USD(A&S) will request that DOT&E certify that the live fire testing and evaluation laid out in the T&E Strategy (or previously in the Live Fire Strategy/Alternative Live Fire Test and Evaluation Plan) is adequate to evaluate the survivability or lethality of the system without using FUSL assets using a combination of component, subsystem and system-level testing, adequately verified and validated M&S tools, and combat, mishap, or safety data where appropriate. DOT&E will provide a memorandum affirming this to be the case, along with the approved Test and Evaluation Master Plan (TEMP), or the appropriate live fire sections of the TEMP, to USD(A&S). In accordance with 10 U.S.C. §§ 4172 (c)(3), USD(A&S) will then submit memoranda and the live fire plan to the chairs and ranking members of the congressional defense committees, informing them of the granting of the waiver.

The waiver package sent to Congress consists of these two parts: 1) certification that the waiver is needed and 2) an approved Alternative LFT&E plan for evaluating survivability or lethality. These two parts require coordination between the acquisition executive USD(A&S) and DOT&E.

3. T&E Documentation

3.1 T&E Strategy to Support T&E Planning

The purpose of T&E planning is to better understand users' needs and define an executable approach to credibly demonstrate the technical, functional, and operational capabilities that need to be delivered to meet users' needs. The planning process is critical and sets the conditions for success. Testing and planning should be digitized and automated as much as possible to support continuous development, integration, and delivery of system capabilities. As such, the PM should establish a common data repository to store T&E data and provide access to all test teams so that they can review, use, and input these test data to meet their objectives. This should enable the use of sequential testing, big data analytics, and other adaptive methods in support of T&E efficiencies.

All test teams should be involved early in the program during the planning process to establish and document how testing, M&S, analysis, and evaluation of the system performance at its various maturity stages will be accomplished. The T&E WIPT and PM should work with the contractor to fully understand the contractor's tools, specifically their verification and validation plans, and the credibility of those tools for the intended use. It is encouraged that government test team train with these tools as appropriate so they can use their outputs to inform evaluations. Such expectations should be clarified with the appropriate contractual provisions.

The PM, in coordination with the T&E WIPT, is responsible for writing the T&E Strategy. The purpose of the T&E Strategy, regardless of the acquisition pathway or naming convention, is to guide the activities of test organizations in planning and executing an effective and efficient test and evaluation process in support of the major program decisions. Common names for T&E strategies may include, but are not limited to, TEMPs, SAMPs, test strategy, and T&E Strategy. This T&E Strategy serves as an agreement between the PM and all the T&E stakeholders for T&E tasks, roles, resources, and responsibilities, and should be developed in the planning phase of the program. The T&E Strategy should be developed in time to inform the acquisition contract and updated as needed across the acquisition cycle to capture the requirements and processes by which systems will be tested and evaluated to verify technical requirements, and to evaluate operational effectiveness, suitability, survivability, and lethality. The T&E Strategy should document the T&E resources required to support DT&E, OT&E, and LFT&E. For programs on T&E oversight, DOT&E is the approval authority of the T&E Strategy. The T&E Strategy for programs not under T&E oversight is approved at the Component level.

The T&E Strategy should be executable and aligned with the Acquisition Strategy, T&E policy (DoDI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. The T&E Strategy will include the Integrated Decision Support Key (IDSK) as per DoDI 5000.89. The T&E Strategy should detail a high-level plan to adequately characterize the performance of the system as it progresses through its major milestones and other critical programmatic decisions. At a minimum, the T&E strategy includes:

- An IDSK that highlights the program decisions and data requirements and sources (e.g., CT, DT, LFT, OT, M&S) to support those decisions, and correlates data requirements with critical operational issues and technical requirements
- Resources and test support requirements needed for all test phases, including consideration for M&S Verification Validation and Accreditation (VV&A) where required
- DT&E, OT&E, and LFT&E scope, objectives, and data
- A program schedule with T&E events and reporting requirements that incorporate report generation timelines
- Test phase objectives, including entrance and exit criteria, cybersecurity test objectives, and M&S events
- Data collection requirements, including from live test events and M&S
- Projected and actual level of funding, including funding sources for all test resources, including M&S VV&A

While a T&E Strategy is the main T&E deliverable for each of the six acquisition pathways, the success of T&E relies heavily on each of the other documents outlined in Table 1. The T&E community should work with the acquisition community on these documents to incorporate needed T&E information. Not all acquisition pathways require all the documentation noted below. For more information on the documents in Table 1, refer to the Milestone Document Identification (MDID) website. The MDID provides a definition of the document, any notes on statutory and/or regulatory requirements, source documents for the specific document, and if applicable, the approval authority. The MDID allows users to filter by program type, life-cycle event, source, and keyword. The acquisition pathway chapters highlight T&E content and involvement of test teams in the development of each of these documents.

Table 1. Documentation Used in T&E Strategy Development

Documentation	Description
Joint Capabilities Integration and Development System (JCIDS) Documentation	The JCIDS process provides the baseline requirements for documentation, review, and validation of capability requirements, at all classification levels, across the Department. JCIDS is the process used by the Joint Requirements Oversight Council (JROC) to fulfill its statutory responsibilities to the Chairman of the Joint Chiefs of Staff (CJCS), including, but not limited to, identifying, assessing, validating, and prioritizing joint military capability requirements. T&E personnel primarily assess the testability, measurability, achievability, and clarity of the capabilities required in the documents, and provide that assessment to the PM and Chief Engineer.

Table 1. Documentation Used in T&E Strategy Development	
Analysis of Alternatives (AoA)	DoDI 5000.84, "Analysis of Alternatives," outlines the procedures, responsibilities, and guidelines for conducting the AoA, which assesses potential materiel solutions that could satisfy the validated capability requirement(s) documented in the Initial Capabilities Document, and supports a decision on the most cost-effective solution to meeting the validated capability requirement(s). In developing feasible alternatives, the AoA identifies a wide range of solutions having a reasonable likelihood of providing the needed capability. AoAs are typically required for programs using the Major Capability Acquisition Pathway, and provide a foundation for the development of documents at the milestones, starting at Milestone A, and is used when developing the T&E Strategy for the preferred solution(s).
Validated Online Life Cycle Threat (VOLT)	The VOLT is the authoritative, system-specific threat assessment tailored for and normally focused on one specific program. The VOLT involves the application of threat modules and is written to articulate the relevance of each module to a specific acquisition program or planned capability. While VOLT reports support Acquisition Category (ACAT) I-III programs, only Major Defense Acquisition Programs (MDAPs) and programs on the T&E Oversight List require a unique, system-specific VOLT report to support capability development. T&E personnel use the VOLT as a reference for developing T&E plans, T&E resources and capability requirements, and test scenarios, as well as a guide for defining the threat environment for a mission-oriented context.
Acquisition Strategy	The Acquisition Strategy is the PM's plan for program execution across the entire program life cycle. It is a comprehensive, integrated plan identifying the acquisition approach and describes the business, technical, and support strategies the PM plans to employ to manage program risks and meet program objectives. The strategy evolves over time and continuously reflects the current status and desired goals of the program. The PM includes the T&E WIPT in the development of the Acquisition Strategy so the T&E Strategy fully supports the program's approach. The Acquisition Strategy includes a description of the test program for both the contractor and the government.
Systems Engineering Plan (SEP)	The Systems Engineering Plan (SEP) documents key technical risks, processes, resources, metrics (Technical Performance Measurement and other metrics), SE products, quality control, and completed or scheduled SE activities. The SEP is a living document, updated as needed to reflect the program's evolving SE approach and/or plans and current status. The purpose of the SEP is to help PMs develop, communicate, and manage the overall SE approach guiding all technical activities of the program. T&E personnel use the SEP as a reference for developing the T&E Strategy, test plans, and other planning documents.
Program Protection Plan (PPP)	In accordance with DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," the PPP describes protection of the system from foreign collection, design vulnerabilities, supply chain exploitation, tampering, and battlefield loss. The Program Office takes an end-to-end system view when developing and executing the PPP (external, interdependent, or government furnished components that may be outside the PM's control should be considered). The PPP provides a usable reference within the program for understanding and managing the full spectrum of program and system security activities. Programs update the PPP as threats and vulnerabilities change or are better understood. T&E personnel use the PPP as a reference for developing the T&E Strategy, test plans, test resource and capability requirements, and other planning documents. The PPP provides information on a program's critical missions, critical functions, critical

Table 1. Documentation Used in T&E Strategy Development	
	components, threats, vulnerabilities, and threat countermeasures. T&E personnel should also consider how Program Protection applies to test events, test processes, and test data, the exploitation of which can cause harm.
Cybersecurity Strategy	In accordance with DoDI 8500.01, "Cybersecurity," the Cybersecurity Strategy describes the program's planned cybersecurity risk management and both the program's long-term approach for, and implementation of, cybersecurity throughout the program lifecycle. All Acquisition programs acquiring systems containing information technology (IT) are required to develop and maintain a Cybersecurity Strategy, which is submitted to the cognizant chief information officer for review and approval at milestones and decision points. The T&E WIPT will review the Cybersecurity Strategy and leverage it in the development of the T&E Strategy.
Security Plan	In accordance with DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," the Security Plan provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The Security Plan should include a system boundary description, implementation status, responsible entities, resources, and estimated completion dates. Security Plans may also include a compiled list of system characteristics or qualities required for system registration, key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The T&E WIPT will review the Security Plan and leverage the details in that plan when developing the T&E Strategy. The details included in the Security Plan can help testers identify specific areas for testing.
Security Assessment Plan	In accordance with DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," a plan to assess the selected security controls must be developed by programs required to follow the Risk Management Framework (which is all DoD information technology that receives, processes, stores, displays, or transmits DoD information). The Security Assessment Plan contains selected controls and their corresponding security control assessment activities with a detailed roadmap of how to conduct such an assessment.
Acquisition Program Baseline (APB)	The APB is the agreement between the MDA and the PM, and the PM's acquisition chain of command, used for tracking and reporting the life of the program or program increment. T&E personnel use the APB as a reference for developing test plans and schedules, test resource and capability requirements, and other planning documents, in an effort to ensure the strategy for T&E remains consistent with the program's goals and objectives. For all ACAT programs, PMs are required to propose and document program goals prior to, and for approval at, program initiation. The MDA will approve entry into the Engineering and Manufacturing Development (EMD) phase and formally initiate the program by approving the APB. All ACAT programs are required to use an APB. For MDAPs, the APB satisfies the requirements in 10 USC 2435 and 2220.
Cost Analysis Baseline Description (CARD)	The DoD conducts analysis to provide accurate information and realistic estimates of cost for DoD acquisition programs, and this data is collected to inform the analysis. Independent and sound cost estimates are vital for effective acquisition decision-making and oversight. For ACAT I and ACAT IA programs, the CARD is used to formally describe the acquisition program for purposes of preparing both the DoD Component Cost Estimate and the Cost Assessment Independent Cost Estimate.

Table 1. Documentation Used in T&E Strategy Development	
	MDAPs and MAIS will provide a CARD in support of major milestone decision points. In accordance with DoDI 5000.73, the PMO will prepare and deliver the draft CARD to the office of Cost Assessment (CA) and the Service Cost Agencies (SCA). For joint programs, the CARD will include the common program agreed to by all participating DoD Components, as well as any unique program requirements of the participating DoD Components. The CDT ensures the test portion of the program definition is sufficiently defined for an adequate estimate. The tester also reviews the cost estimates resulting from the CARD to ensure reasonable funding and that the funding is included in the Resources section of the T&E Strategy. Finally, cost estimates for testing eventually appear in the Research, Development, Test & Evaluation (RDT&E) Exhibits (specifically R-2 and R-3 for test), which go to the President and Congress, and the T&E Budget Submissions (T&E-1), which go to the DoD.
Lifecycle Sustainment Plan (LCSP)	The LCSP describes sustainment influences on system design and the technical, business, and management activities to develop, implement, and deliver a product support package that maintains affordable system operational effectiveness, suitability, survivability and/or lethality over the system life cycle, and seeks to reduce cost without sacrificing necessary levels of program support. According to IAW DoDI 5000.85, "Major Capability Acquisition," DoD Components will ensure reliability and maintainability data from operational and developmental testing and evaluation, fielding, all levels of repair and their associated manpower, and real property informs estimates Operations and Support costs for major weapon systems.
Information Support Plan (ISP)	The ISP serves as a key document in achieving interoperability certification. The ISP describes IT and information needs, dependencies, and interfaces for programs in all acquisition categories. It focuses on the efficient and effective exchange of information that, if not properly managed, could limit or restrict the operation of the program from delivering its defined capability. The Net-Ready Key Performance Parameter (NR-KPP) identified in the CDD will also be used in the ISP to identify support required from external information systems. Bandwidth requirements data will also be documented in the ISP. T&E personnel use the ISP to identify how the system should be tested to evaluate 1) users' ability to enter and manage a network, 2) users' ability to exchange information, and 3) how the system supports military operations. T&E personnel can use the ISP and a CONOPS/OMS/MP to develop test scenarios for evaluating key information/data exchanges that have an impact on mission success.
Lifecycle Mission Data Plan (LMDP)	In accordance with DoDD 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition" are required for IMD-dependent programs. IMD are defined as DoD intelligence-derived information used for programming platform mission systems in development, testing, operations, and sustainment, including, but not limited to, the following functional areas: intelligence signatures, electronic warfare integrated reprogramming (EWIR), order of battle (OOB), characteristics and performance (C&P), and geospatial intelligence (GEOINT). The LMDP defines specific IMD requirements for a program, and becomes more detailed as the system progresses toward IOC. During development of T&E strategies and plans, IMD requirements are identified based on the need to verify and validate detection and identification functionality for DT&E, and for operational effectiveness, suitability, and survivability for OT&E. The T&E Strategy should define specific intelligence requirements to support program developmental and operational test and

Table 1. Documentation Used in T&E Strategy Development	
	evaluation. The LMDP should include information on IMD data existing within the program for sensor or algorithm development, or for testing purposes.
Request for Proposal (RFP)	A Request for Proposal (RFP) is a solicitation used in negotiated acquisition to communicate government requirements to the prospective contractors and to solicit proposals. At a minimum, solicitations shall describe the T&E community test requirements, anticipated terms and conditions that will apply to the contract, information required in the offeror's proposal, and (for competitive acquisitions) the criteria that will be used to evaluate the proposal and their relative importance.

3.2 Test Plans

The lead test organization, in coordination with the T&E WIPT, develops test plans for each event identified in the T&E Strategy. For any events that may affect safety of personnel, the T&E community, working with the PM and user community, will provide relevant safety documentation. Barring unforeseen circumstances, all elements of an approved test plan should be satisfied by the end of the test period, including collection of all required data. Test plans should include information about the order of test event execution and test data collection, as well as relevant operating instructions that may impact test outcomes. At a minimum, test plans should detail:

- Test purpose in relation to overall T&E Strategy and program life cycle
- Test schedule, location, and resources (personnel, targets, threat)
- Data requirements and how the test team will collect, reduce, and distribute data
- Test limitations

For programs on the T&E oversight list, operational test plans across all acquisition pathways, including LFT&E strategies, must be approved by DOT&E and should be submitted to DOT&E at least 60 days prior to the start of testing. If the test cannot be executed according to the approved plan, DOT&E concurrence must be obtained prior to executing revised test events.

4. T&E Organizations

4.1 Office of the Secretary of Defense (OSD) Test & Evaluation Organizations

4.1.1 Under Secretary of Defense for Research and Engineering (USD(R&E))

The USD(R&E) is the principal advisor to the Secretary and Deputy Secretary of Defense for all matters regarding the DoD Research and Engineering (R&E) Enterprise, defense R&E, technology development, technology transition, developmental prototyping, experimentation, developmental testing activities and programs, and unifying defense R&E efforts across the DoD. As outlined in DoDI 5000.89, the USD(R&E):

1. Establishes policies and strategic guidance and leads defense research; engineering; developmental prototyping and experimentation; technology development, exploitation, transition, and transfer; DT&E; and manufacturing technology activities
2. Prepares Milestone B and Milestone C DT&E sufficiency assessments on Major Defense Acquisition Programs (MDAPs) where the Defense Acquisition Executive (DAE) is the MDA
3. Develops DT&E policy and ensures appropriate test facilities, test ranges, tools, and related M&S capabilities are maintained within the DoD
4. Serves as an advisor to the Joint Requirements Oversight Council on matters within USD(R&E) authority and expertise to inform and influence requirements, concepts, capabilities-based assessments, and CONOPS
5. Approves the DT&E plan within TEMPs and delegates approval authority, as appropriate
6. Develops governing policy and advances practices and workforce competencies for DT&E

4.1.1.1 Director, Developmental Test, Evaluation & Assessments (D(DTE&A))

The D(DTE&A) serves as the principal advisor to the USD(R&E) for developmental test, evaluation, and assessments, and supports the USD(R&E) in the conduct of its T&E responsibilities and activities listed in Section 2.1.1. The D(DTE&A) provides system engineering (SE) and T&E rigor to DoD Adaptive Acquisition Framework (AAF) pathways and R&E modernization priorities to ensure delivery of relevant and timely warfighting capabilities by:

- Engaging AAF and early prototyping programs in developing innovative and efficient DT&E and SE strategies supporting acquisition life-cycle decisions that deliver capability advantages needed by warfighters
- Providing independent DT&E, Engineering, and Technical Risk Assessments to accurately evaluate technical performance and technology, engineering, and integration maturity in support of critical decisions
- Supporting the development and implementation of T&E and SE policy and guidance for the acquisition life-cycle continuum

4.1.1.2 Test Resource Management Center (TRMC)

The Director Test Resource Management Center (TRMC) serves as the principal advisor to the USD(R&E) on matters pertaining to strategic planning and assessment of the DoD T&E infrastructure.. The TRMC provides robust and flexible T&E capabilities to develop, acquire, field, and sustain reliable and effective weapons systems to meet the current and future needs of the warfighter. It looks across the entire T&E infrastructure to align T&E efforts with DoD modernization goals and ensure ranges are ready to test new capabilities as they emerge.

The TRMC oversees the Major Range and Test Facility Base (MRTFB), plans for and assesses the adequacy of the MRTFB, and maintains awareness of other T&E facilities and resources, within and outside the Department, and their impacts on DoD requirements (DoDD 5105.71, March 8, 2004, Section 4).
The TRMC accomplishes its missions through the:

Major Range and Test Facility Base. The MRTFB is the designated core set of DoD T&E infrastructure (open-air ranges, test facilities, instrumentation data processing, and other test resources) and associated workforce to provide T&E capabilities in support of the DoD acquisition system (DoDD 3200.11, Change 2 October 15, 2018, Paragraph 3); it operates in accordance with DoDI 3200.18, Change 2 October 15, 2018.

Central T&E Investment Program (CTEIP). CTEIP provides OSD funding and a mechanism for the development and acquisition of new test capabilities to satisfy multi-Service requirements. It administers the acquisition and integration of all training and associated test range instrumentation and development-related policy by:

- Addressing modernization projects too large for a single Service
- Ensuring requirements solve multi-Service needs
- Developing integrated solutions across the spectrum of T&E capabilities
- Developing common range instrumentation that benefits many platforms (DoDD 3200.11 Change 2, October 15, 2018)

T&E Science and Technology (T&E/S&T) Program. The T&E/S&T Program develops test technologies to keep pace with evolving weapons technologies. Funded within the Advanced Technology Development Budget Activity, the T&E/S&T Program is critical to ensuring DoD ability to adequately test advanced systems that will be fielded in the future. T&E/S&T Program technology development projects typically begin at Technology Readiness Level (TRL) 3 and mature to TRL 6; deliverables include test technology prototypes and demonstrations in relevant test environments. The T&E/S&T Program addresses long-term gaps in the T&E infrastructure, as well as risk reduction for the development of test capabilities.

The TRMC manages the T&E/S&T Program, which employs a decentralized execution process through Test Technology Areas, each of which is led by an Executing Agent from one of the Services and based at a test organization in the field. Each Executing Agent leads a working group composed of representatives from the DoD T&E and S&T communities, with expertise related to the respective test technology.

Joint Mission Environment Test Capability (JMETC) Program. JMETC provides a persistent capability for linking distributed facilities, enabling DoD customers to develop and test warfighting capabilities in a joint context. JMETC provides a test infrastructure consisting of the components necessary to conduct joint distributed test events by cost-effectively integrating live, virtual, and constructive test resources configured to support users' needs. The JMETC program provides customers with a support team to assist with JMETC products and the conduct of distributed testing.

National Cyber Range Complex (NCRC) Program. The NCRC improves the resiliency and lethality of the nation's warfighters in the cyber-contested battlespace by delivering operationally representative cyberspace environments for T&E, training, and mission rehearsal. The NCRC team supports DoD acquisition program managers in the planning and execution of a wide range of cybersecurity activities throughout the lifecycle, including science and technology experimentation, architectural evaluations, security control assessments, cooperative vulnerability and penetration assessments (CVPA), and adversarial assessments (AA). The NCRC supports training, certification, and mission rehearsal requirements for the Cyber Mission Force (CMF).

Test Resource – Governance (TR-G) Division. The TR-G Division advises the Director, TRMC on MRTFB policy, workforce, infrastructure changes, budgets, and expenditures, with the goal of ensuring that the MRTFB maintain a broad base of T&E capabilities sufficient to support the full spectrum of DoD T&E requirements.

Test and Training Enabling Architecture (TENA) Software Development Activity (SDA). TENA provides the architecture and software implementation necessary to:

- Enable interoperability among range systems, facilities, simulations, and command, control, communications, computers (C4) intelligence, surveillance, and reconnaissance (ISR) systems in a quick, cost-efficient manner
- Foster reuse for range asset utilization and for future developments
- Provide composability to rapidly assemble, initialize, test, and execute a system from a pool of reusable, interoperable elements

4.1.2 Director, Operational Test and Evaluation (DOT&E)

The DOT&E is the principal adviser to the Secretary of Defense, the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), and the Under Secretary of Defense for Research and Engineering (USD(R&E)) on OT&E and LFT&E in the DoD, and the principal OT&E and LFT&E official within the senior management of the DoD. The DOT&E:

1. Prescribes policies and procedures for the conduct of OT&E and LFT&E for the DoD across the acquisition pathways
2. Monitors and reviews OT&E and LFT&E activities in the DoD
3. Oversees MDAPs or other programs designated by the Director for T&E oversight
4. Determines specific OT&E and LFT&E policy and best practices for each of the acquisition pathways, as applicable
5. Designates select programs for DOT&E operational and live fire oversight in accordance with 10 U.S.C. §§ 139, 4171, 4172, and 4231, as applicable, and the criteria outlined in Paragraph 3.2 of DoDI 5000.89
6. In coordination with the USD(R&E), jointly publishes and manages the T&E Oversight List, which identifies all programs under oversight for DT&E, OT&E, or LFT&E

7. Approves the OT&E and LFT&E planned activities in TEMPs, test strategies, or other overarching program test planning documents for programs on the T&E oversight list
8. Approves, in writing, the adequacy of OT and LF plans for those programs under T&E oversight before OT or LF begins
9. Approves alternative LFT&E plans and strategies for evaluating survivability or lethality when a waiver from FUSL testing is being sought, in accordance with timelines established in 10 U.S.C. §§ 4172
10. Determines the quantity of articles to be procured for operational and live fire test for systems on the T&E oversight list for operational and/or live fire testing
11. Evaluates and approves the use of production-representative articles for purposes of adequate and realistic initial operational test and evaluation (IOT&E) for programs under T&E oversight for operational and/or live fire testing
12. Assesses the adequacy of OT&E and LFT&E performed by the Services and operational test agencies (OTAs) for programs under T&E oversight for operational and/or live fire testing
13. Approves, in writing, the use of data collected outside an approved operational test plan (OTP) for use in operational evaluation for programs under T&E oversight for operational and/or live fire testing
14. Submits independent OT&E and LFT&E reports to the OSD, Joint Staff, DoD Components, and congressional defense committees, as applicable
15. Submits a report after the conclusion of OT&E and LFT&E, as required by 10 U.S.C. §§ 4171, 4172, to the OSD, Joint Staff, DoD Components, and congressional defense committees before systems under T&E oversight may proceed to beyond LRIP
16. Submits an annual report summarizing the operational and live fire test and evaluation activities of the Department of Defense during the preceding fiscal year as required by 10 U.S.C. §§ 139(h)

In accordance with DoDD 5141.02, DOT&E is responsible for ensuring the stability in funding and strategic guidance for the following joint DOD activities intended to further assess and enhance the operational performance of the warfighter in combat.

4.1.2.1 Joint Test and Evaluation (JT&E) Program

The JT&E Program enables the planning and execution of joint tests to support the future fight. The JT&E Program considers emerging technologies and the increasingly complex and dynamic, joint, multi-domain operational environment to develop solutions intended to enhance the United States' operational effectiveness, suitability, and survivability in combat. As the Services and Combatant Commands (CCMD) help identify critical challenges that need to be addressed in their areas of responsibility to maintain superiority across joint, multi-domain operations, the JT&E Program provides operational test and evaluation management and expertise to develop, test, and validate joint solutions, including agile warfighting tactics, techniques, and procedures (TTPs),

concepts of employment (CONEMP), and concepts of operations (CONOPS). Given the increased integration and dependencies of platform, network, and command and control solutions across the domains, JT&E's mission and unique focus on system of systems testing is becoming increasingly critical to the Department's strategic objectives, to include modernization. JT&E test techniques, workforce talents, and reach-back are essential to the adequate evaluation of the effectiveness of operational plans across the CCMDs.

4.1.2.2 Joint Live Fire (JLF) Program

The JLF Program's primary mission is to enable the development of adequate LFT&E tools, methods, and infrastructure, to include digital technologies needed for credible evaluation of DoD systems' survivability and lethality and development and validation of Joint Munitions Effectiveness Manuals (JMEMs) and weaponeering tools. The JLF Program is focused on addressing survivability/lethality T&E capability shortfalls due to the increased complexity of DoD systems and adversary threats.

4.1.2.3 Center for Countermeasures (CCM)

The CCM is a joint activity focused on the planning and execution of T&E activities intended to evaluate the operational effectiveness of countermeasures and counter-countermeasures employed by a range of DoD and foreign weapon systems. It accomplishes this by operating and deploying mobile test equipment capable of simulating an array of adversarial threats throughout the country. The transportability of CCM test tools and personnel provides the requisite test agility and efficiency for the DoD to develop and field warfighting capability at operationally relevant speeds. It minimizes the deployment of aircraft and Program Office staff to test locations, preserving their schedules and resources. CCM supports system developers and Service developmental and operational test agencies in the T&E of DoD systems.

4.1.2.4 Joint Aircraft Survivability Program (JASP)

The JASP Program develops cross-Service aircraft survivability solutions and evaluation methods needed to dominate the multi-domain battlefield and mitigate U.S. aircraft losses in combat. JASP products support: 1) weapons tactics schools, air operations, and training, 2) operational and live fire test and evaluation of aircraft systems, 3) aircraft combat damage reporting, and 4) transition of technologies to the battlefield intended to improve aircraft survivability and force protection. The Services' aviation acquisition commands (Army Aviation and Missile Command (AMCOM), Air Force Life Cycle Management Center (AFLCMC), and Naval Air Systems Command (NAVAIR)) depend on JASP activities to increase U.S. military aircraft combat effectiveness in current and emerging threat environments through the joint coordination and development of T&E capability and aircraft survivability technologies that complement Service aircraft survivability programs. JASP efforts include RDT&E of susceptibility and vulnerability

reduction technologies, M&S, aircraft combat damage reporting, and aircraft survivability education.

4.1.2.5 Joint Technical Coordinating Group for Munition Effectiveness (JTCG/ME)

The JTCG/ME program develops validated weaponeering tools for multi-domain operations derived from the policy-approved Joint Munition Effectiveness Manuals (JMEMs). Combatant Command strike authorities rely on these weaponeering tools to estimate and optimize the type and number of U.S. weapons or capabilities required to achieve the desired lethal effect against a range of strategic or tactical targets while mitigating risk for collateral damage, to include civilian casualties. DOT&E provides oversight, stability in funding, and strategic guidance, while the Army's Combat Capability Development Command Data and Analysis Center (DEVCOM DAC) executes the JTCG/ME mission in accordance with DOT&E guidance, JTCG/ME Executive Steering Committee guidance, Joint Staff Military Targeting Committee requirements, and Chairman of the Joint Chiefs of Staff instructions.

4.1.2.6 Test and Evaluation Threat Resource Activity (TETRA)

TETRA is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA) established to ensure that OT&E and LFT&E programs and warfighter training are adequately informed by the latest and emerging intelligence data. TETRA manages a Threat Systems Database cataloging asset availability, location, limitations, and adequacy, and continues to enhance its support to the OT&E community by identifying significant system vulnerabilities and evaluating their operational impacts, underpinning DOT&E's role in fielding the most effective and suitable equipment to the warfighter. TETRA's T&E Threat M&S Configuration Management System implements controls and distribution management for threat M&S products. TETRA, working with Intelligence Production Centers and acting as the DOT&E lead for Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects, evaluates options to build threat-representative simulators and models from intelligence, open source, and industry data. TETRA also provides oversight of the Services' threat verification and validation process, which confirms that a system meets design specifications and documents the differences between actual threat performance and that of the representation. TETRA also represents DOT&E in the Foreign Materiel Program overseen by the Office of the Under Secretary of Defense for Intelligence and Security. The objective of TETRA's involvement in the Foreign Materiel Program is to secure actual systems for intelligence analysis and use in operational testing. Additionally, TETRA developed and continues to maintain the Threat Systems Database, which catalogs threat assets available for the T&E community.

4.1.2.7 International Test and Evaluation Program (ITEP)

ITEP enables bilateral and multilateral agreements between U.S. forces and Allies which are critical for expediting the development and fielding of advanced warfighting technologies, and supporting T&E infrastructure and capabilities. These agreements

enable the planning and execution of cooperative T&E projects, transfer of necessary test equipment and materials, exchange of T&E-relevant information through working groups, and reciprocal use of test facilities. ITEP fulfills the requirement to test in natural environments not available in the U.S., provides access to technical test capabilities the U.S. does not have or are out of service, and provides for partner access to U.S. ranges and facilities when needed.

4.1.2.8 Cyber Assessment Program (CAP)

DOT&E also manages and fully funds the CAP, which was created in response to a conference report in the FY03 NDAA to "monitor the DoD's ongoing efforts to improve interoperability and information assurance." CAP is planned and executed with the Combatant Commands, Services, Operational Test Agencies, DoD-certified Red Teams, and the Intelligence Community. Current mission priorities include: 1) mission-focused operational assessment using validated and persistent cyber threats, 2) assessment of warfighter ability to execute missions in a contested environment, 3) identification of critical vulnerabilities, facilitation or remediation, and verification, and 4) assistance to cyber defender personnel to improve detections and responses to cyber attack.

4.2 DoD Component T&E Organizations

4.2.1 Department of the Army

4.2.1.1 Department of the Army T&E Executive

The Army T&E Executive is the Director, T&E Office under the authority, direction, and control of the Deputy Under Secretary of the Army, and:

- Serves as the senior advisor to the Secretary of the Army and Army Chief of Staff on all Army T&E matters
- Advises the Army Systems Acquisition Review Council (ASARC), the Army Requirements Oversight Council (AROC), and Overarching Integrated Product Teams (OIPTs) on T&E matters
- Approves test-related documentation for the Secretary of the Army and forwarding, as appropriate, to OSD
- Coordinates T&E matters with the Joint Staff and OSD, including serving as the principal Army interface on T&E matters with the USD(R&E) and DOT&E
- Oversees all Army T&E missions and functions, to include formulating overarching Army T&E strategy, policy, and program direction, providing policy oversight, and management of resources
- Provides Headquarters, Department of the Army oversight on the funding of the Army Threat Simulator program, Army Targets program, and Army Instrumentation program

- Oversees Army responsibilities in Joint T&E, Foreign Comparative Testing (FCT), and multi-Service and multi-national T&E acquisition programs
- Serves as the Army T&E functional chief for the T&E acquisition workforce career field (Army Regulation 73-1, June 8, 2018, Section 2-18)
- Serves as the Chemical and Biological Defense Program (CBDP) T&E Executive in accordance with DoDD 5160.05E, Paragraph 2.14.d (Change 2 July 18, 2019
- Oversees the adequacy of T&E programs and infrastructure that supports the CBDP test requirements

4.2.1.2 U.S. Army Test and Evaluation Command (ATEC)

ATEC is the Army's OTA and consists of the U.S. Army Evaluation Center (AEC), U.S. Army Operational Test Command (OTC), and Test Centers. AEC produces independent, comprehensive evaluations and assessments by consolidating all developmental and operational testing and other credible data to provide essential information to decision makers. AEC also produces system safety documentation. OTC plans, conducts, and reports on operational tests to provide essential information to AEC. ATEC's Test Centers plan, conduct, and report on developmental tests to provide essential information to AEC (Army Regulation 73-1).

4.2.2 Department of the Navy

4.2.2.1 Department of the Navy (DON) T&E Executive

For the purpose of this instruction, DON T&E will be used to indicate responsibilities for both the DON T&E Executive and the Director, Innovation, Test & Evaluation, and Technology Requirements (OPNAV N94). Specific DON T&E responsibilities include:

- Establish and implement DON DT&E, LFT&E, and OT&E policy for the various DoD-defined AAF pathways within the DON
- Coordinate development and implementation of Capability-Based Test and Evaluation (CBTE) processes to integrate T&E phases into a single T&E continuum
- Endorse or approve DON TEMPs and MTS for all Navy programs and USMC ACAT I programs, BCAT I programs requiring OT, and programs on oversight
- Act for the SECNAV, CNO, and CMC as the senior DON representative responsible for coordination with DOT&E and Director, Developmental Test, Evaluation and Assessment (D, DTE&A) for T&E policy issues and acquisition program TEMP, DT, OT, and LFT&E matters
- Establish the TECP for identifying, tracking, and resolving program T&E issues
- Determine, with SYSCOM and Service OTA support, the adequacy of T&E infrastructure and coordinate infrastructure investment required to support systems testing

- Coordinate DON participation in testing of Joint programs
- Review requirements capabilities documents (e.g., Initial Capabilities Document (ICD), CDD and CDD updates, CNS)
- Establish process for coordinating Fleet assets for T&E support
- Oversee testing matters associated with Marine Corps equipment, and ensure integration of Navy and USMC testing for USMC systems deployed on Navy ships
- Support scheduling fleet resources for RDT&E efforts
- Coordinate target resource planning with program resource sponsors, and procure and allocate Naval targets for training and T&E claimants
- Assist CDT/T&E leads in implementation of elements of this instruction and accompanying guidebook (Each DON acquisition program is assigned to a specific N942 Action Officer (AO) responsible for assisting the CDT/T&E lead with implementing elements of this instruction and the guidebook and obtaining RDT&E resources to support their T&E efforts; the list of AO portfolios can be found at the DON Acquisitions T&E Collaboration SharePoint Site.)
- Chair a T&E Requirements and Resources Board (TERRB) for MCA programs prior to Gate 3/MDD and each program/capability modification initiation to support the Gate/initiation (The TERRB will use System Capability Requirements and OTA-developed system-specific mission tasks/conditions analysis to assess the availability and resourcing of required T&E infrastructure (including a gap assessment), as well as establishing the demand and funding for resources such as targets, missiles, ranges, and M&S. Assessment of adequacy of resources and identification of gaps will be briefed at the Gate/Program initiation brief, and support initial TEMP development.)

4.2.2.2 U.S. Navy Operational Test and Evaluation Force (OPTEVFOR)

The Navy COMOPTEVFOR provides independent and objective assessments for the effectiveness, suitability, survivability and/or lethality of naval aviation; surface; subsurface; command, control, communications, computers, and intelligence (C4I); cryptologic; and space systems in support of DoD and Navy acquisition and fleet introduction decisions (SECNAVINST 5000.2F).

4.2.2.3 U.S. Marine Corps Operational Test and Evaluation Activity (MCOTEA)

MCOTEA provides OT&E for the Marine Corps and conducts additional T&E as required to support the Marine Corps mission to man, train, equip, and sustain a force in readiness. Further information on MCOTEA can be accessed here.

4.2.3 Department of the Air Force

4.2.3.1 Air Force T&E Executive

The Air Force T&E Executive is Director, Air Force Test and Evaluation (AF/TE) and:

- Functions as the focal point for Air Force T&E policy, guidance, direction, and oversight for the formulation, review, and execution of T&E plans, programs, and budgets
- Functions as the chief T&E advisor to senior Air Force leadership on T&E processes, including contractor testing, DT&E, OT&E, LFT&E, and the use of M&S in T&E
- Functions as the final T&E review authority and signatory for TEMPs prior to the Service or the Component Acquisition Executive and OSD approval and signature
- Collaborates with requirements sponsors and system developers to improve operational requirements, system development, and the fielding of operationally effective, suitable, safe, and survivable systems
- Oversees the Air Force T&E infrastructure by determining the adequacy of T&E resources required to support system acquisition activities
- Administers various T&E resource processes and chairs or serves on various committees, boards, and groups supporting T&E activities
- Manages the Air Force Joint Test and Evaluation program according to DoDI 5010.41, "Joint Test and Evaluation (JT&E) Program" *(*HAF MD 1-52)

4.2.3.2 U.S. Air Force Operational Test and Evaluation Center (AFOTEC)

AFOTEC is the Air Force's independent test agency responsible for testing, under operationally realistic conditions, new systems being developed for Air Force and multi-service use. AFOTEC's independent and objective evaluations of how well systems will meet operational requirements provide a vital link between the developer and user. Further information on AFOTEC can be accessed here.

4.2.3.3 Space Training and Readiness Command (STARCOM)

STARCOM exists to prepare combat-ready United States Space Force (USSF) forces to fight and win in a contested, degraded, and operationally-limited environment through the deliberate development, education and training of space professionals; development of space warfighting doctrine, tactics, techniques, and procedures; and the test and evaluation of USSF capabilities. (At the time of the issuance of this chapter, AFOTEC is in the process of transitioning test and evaluation of USSF to STARCOM.)

4.2.4 Defense Information Systems Agency (DISA)

4.2.4.1 DISA T&E Executive

The DISA T&E Executive is the Commander, Joint Interoperability Test Command (JITC). DISA is a combat support agency of the DoD and provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations. Further information on DISA can be accessed here.

4.2.4.2 Joint Interoperability Test Command (JITC)

The Joint Interoperability Test Command (JITC) is the only non-Service OTA for Information Technology (IT)/National Security Systems (NSS). JITC provides an independent and objective evaluation for the operational effectiveness, suitability, and survivability (cyber) in support of DISA and other DoD agency acquisition decisions. JITC, as the DoD's Joint Interoperability Certifier, also provides interoperability assessments in support of Operational Test Readiness Reviews. Further information on JITC can be accessed here.

5 T&E Program Management

5.1 Program Manager (PM)

The PM is responsible for building, executing, and resourcing a rigorous and robust T&E program. To the extent possible, the PM should work with the T&E community to inform the requirements, acquisition contracts, and source selections and to construct a T&E Strategy.

5.2 T&E Working Integrated Product Team (T&E WIPT)

The PM should charter a T&E WIPT to translate the T&E Strategy into the appropriate test strategy documentation. The T&E WIPT consists of representatives from all organizations responsible for providing for or overseeing the T&E Strategy and its execution. In particular, the T&E WIPT should include stakeholders such as systems engineers, developmental testers, operational testers, live fire testers, the user, product support, the Intelligence Community, cybersecurity experts, and applicable certification authorities. The T&E WIPT may also split into sub-WIPTs as appropriate to address specific focus areas (e.g., live fire, cyber, and RAM).

5.3 Chief Developmental Tester (CDT)

As soon as practical, after establishing the program, the PM should designate a CDT. The CDT will be responsible for coordinating the planning, management, and oversight of all

DT&E (contractor and government) activities; overseeing the T&E activities of other participating government activities; and helping the PM make technically informed, objective judgments about contractor and government T&E planning and results.

5.4 Lead DT&E Organization

PMs will designate, as soon as practicable after the Program Office is established, a Lead DT&E Organization, which will be responsible for 1) providing technical expertise on T&E concerns to the CDT, 2) conducting DT&E activities to support independent evaluations and as directed by the CDT or their designee, 3) supporting certification and accreditation activities, and 4) assisting the CDT in providing oversight of contractors and in reaching technically informed, objective judgments about contractor and government T&E planning and results.

5.5 Lead Operational Test Agency (OTA)

OTAs provide DOT&E plans to assess the adequacy of data collection and analysis planning to support the DOT&E's independent assessment of a system's operational effectiveness, suitability, survivability, and lethality.

6 T&E Oversight List

The DOT&E and the USD(R&E)) publish a joint T&E Oversight List in accordance with DoDI 5000.89, which includes acquisition programs designated for DT, OT, and LFT&E oversight. The T&E Oversight List does not include highly classified and sensitive programs. DOT&E and USD(R&E) identify the oversight of such programs directly to the Service or the Component Acquisition Executives. DOT&E maintains the T&E Oversight List, designated Controlled Unclassified Information (CUI), which can be accessed here using a common access card. DOT&E and USD(R&E) will continuously review and update the oversight list and notify each other and the Services accordingly.

As USD(A&S) and Service or the Component Acquisition Executives identify new acquisition programs for any of the six acquisition pathways in accordance with DoDI 5000.02, DOT&E will apply the following criteria to determine the need for OT and LFT&E oversight:

- Program exceeds or has the potential to exceed the dollar value threshold for a major program, to include MDAPs, designated major subprograms, as well as highly classified programs and pre-MDAPs
- Program has a high level of Congressional or DoD interest
- Weapons, equipment, or munitions that provide or enable a critical mission warfighting capability or is a militarily significant change to a weapon system

Additionally, DOT&E will consider the following to determine when programs should be removed from DOT&E oversight:

- T&E (initial and follow-on OT&E and/or LFT&E) is complete, and associated reporting to inform fielding and full-rate production decisions is complete
- Program development has stabilized and there are no significant upgrade activities

In accordance with DoDI 5000.89, DOT&E is the approval authority for TEMPs, test strategies, and other overarching program test planning documents for all programs on the T&E oversight list for OT and LF.
The USD(R&E) will apply the following criteria to determine the need and priority for DT&E oversight:

- ACAT ID programs, pre-MDAP ACAT ID programs, and ACAT ID Defense Acquisition Executive-designated Special Access Programs
- Missile system programs and associated equipment that are an integral part of the layered and integrated Missile Defense System for homeland and regional defense
- Adaptive Acquisition Framework programs that are national security systems providing intelligence activities, cryptographic activities related to national security, and command and control of military forces
- Programs with open or unresolved high technical risk rated areas as determined by an Independent Technical Risk Assessment
- ACAT IB and IC programs conducting DT&E activities prior to Initial Operational Test and Evaluation (IOT&E) or Follow-on Operational Test and Evaluation (FOT&E) to verify a military capability:
  - Directly linked to the successful execution of an ACAT ID program CONOPS
  - Supporting a USD(R&E) Assistant Director Modernization Road Map or investment area
  - Receiving high-level interest and attention as communicated by Congressional or Department principals
- In coordination with USD(A&S), critical 804 Middle Tier of Acquisition Programs

USD(R&E) reviews and approves DT&E plans (in the TEMP, test strategy, or other overarching program test planning documents) for ACAT ID programs. For other programs on oversight for DT&E (e.g., ACAT IB and IC), USD(R&E) reviews and advises the Milestone Decision Authority on the adequacy of such plans.

7 Phases of T&E

T&E phases, as listed in the T&E Competency Model on the DAU website, are planning, preparation, execution, analysis, valuation, and reporting. General information about each phase is listed below.

T&E Phase	T&E Activities
Planning	Support the development of system requirements and acquisition contracts (Not found in T&E competency model. Inserted for the purposes of T&E guidance only. • Identify T&E risk factors based on likelihood and consequence of occurrence to test strategy/approach and impact on the overall program

T&E Phase	T&E Activities
	plan and schedule through participation in all program risk management processes. • Develop risk mitigation recommendations for T&E risk factors in accordance with the processes and procedures found in the DoD Risk, Issue, and Opportunity Management Guide to cover system risk elements throughout the acquisition cycle and during the test program. • Support Program Management Office's development of a risk management plan with T&E-relevant risks and mitigation plans that enable a balanced plan for a program. • Translate requirements documents to identify evaluation criteria to support T&E planning. • Determine whether the capability requirements are sufficiently defined to assess testability and that they are relevant to the operational mission. Understand how flexible requirements in agile developments could affect T&E. • Determine data requirements to assess evaluation criteria for assessing the system performance requirements and evaluation of Critical Operational Issues, Key Performance Parameters, and Key System Attributes. • Determine necessary T&E infrastructure requirements and identify shortfalls that will require investments to meet T&E infrastructure sufficiency, and if and how the Digital Engineering Ecosystem is being used for the program. • Apply all T&E policies, practices, and procedures to develop a T&E Strategy that supports the program's Acquisition Strategy for the applicable Adaptive Acquisition Pathway. Incorporate IT at the earliest opportunity and identify how the following components fit together during systems development: CT, DT, OT, and LFT. For T&E aspects, identify where interoperability, cybersecurity, Scientific Test and Analysis Techniques (STAT), environmental mitigation, safety, and mission-level testing, etc., fit into system development. Determine the appropriate criteria for evaluating OT parameters (Effectiveness and Suitability) and LFT&E parameters (Lethality and Survivability). • Document the T&E Strategy that integrates policy, program requirements, cost and resource estimates, evaluation framework, and the T&E schedule to accomplish program goals. Use appropriate contracting strategies to maximize the efficient use of human capital and other resources. • Identify all organizations and activities with roles and responsibilities in providing for or overseeing the T&E Strategy that supports a program’s acquisition life cycle or a system of systems' acquisition life cycle. • Identify and organize the T&E management forum (e.g., T&E WIPT, Integrated Test Team, Combined Test Team) necessary to address all T&E issues and documentation to support the T&E Strategy, approach, and overall program plan. • Translate the T&E Strategy into the appropriate test planning documentation (e.g., Developmental Test Plans, Operational Test Plans, and Live-Fire Test Plans) including identification of all the required resources to ensure the strategy is executable and supports the Systems Engineering Plan and overall Acquisition Strategy.

T&E Phase	T&E Activities
	• Provide financial cost estimates for T&E support to ensure resources are available and mapped against the schedule to ensure availability during development and production of the system life cycle. Ensure all test costs are fully captured in budget requests and TEMP resource tables, or other test strategy documentation.
Preparation	• Interact with all organizations/activities that require information/activity exchange to successfully complete the test planning as enumerated in the T&E Strategy. • Continually coordinate and monitor availability of required test and/or evaluation resources to identify any potential resource problem to ensure effective completion of test events. • Execute tasking orders and funding streams to commit resources as requested, when and where required to complete T&E activities/events. Ensure accounting of all applicable T&E resources. • Verify readiness of resources for T&E program execution. • Ensure all required resources are deployed to the test site(s) as required and in sufficient time to provide for pre-test rehearsal(s), communications, and instrumentation checks. • Comply with and implement policies and procedures (e.g., safety, security, environmental) required to successfully conduct test activity/event. • Investigate specific policies, procedures, and operational constraints for applicable test ranges to ensure compatibility during test operations. • Assess all T&E related factors to determine system/test article readiness before starting the test. Ensure adequate personnel are assigned to allow continual coverage for overlapping test events. • Plan, conduct, and report on Test Readiness Reviews.
Execution	• Manage test execution/risk mitigation factors by adapting to real-time changes/challenges to advise Test Director to optimize test opportunity and coverage of key parameters/factors/conditions that have significant effect(s) on operational performance. • Confirm data collection tools are valid, operators and maintainers are trained, M&S/Live Virtual Constructive hardware and software tools are properly integrated, and system under test is configured as required to execute the test events/activities and collect required data. • Confirm and monitor security and safety compliance (such as people and item/system under test) and environmental requirements/constraints to protect resources and comply with established policies. • Develop, validate, rehearse, and execute tests in an organized fashion to facilitate identification of completed data suitable in form and format for analysis and evaluation. Ensure data required for STAT analysis are suitable. • Control the test schedule to ensure timely execution of critical tasks, assigned resources, and project milestones to optimize collection of data in support of evaluation objectives. • Verify all required and expected raw test data to ensure completeness of data to support a system evaluation.

T&E Phase	T&E Activities
	• Ensure validity of collected test data to meet test objectives in support of planned analysis and evaluation. Determine how cybersecurity will be used to protect the integrity of test data. • Distribute data per the data management plan for analysis of test results in support of the evaluation.
Analysis	• Translate outputs from test instrumentation systems, data acquisition system methods and formats, software tools/logs, capabilities, and operation to verify and validate test data set. • Identify gaps and variances in raw test data to determine data voids or outliers that may degrade analysis and evaluation. • Reduce, translate, and analyze raw test data into organized and meaningful data products to support planned analysis of STAT-based design, evaluation, and reporting. • Conduct data scoring to refine demonstrated test results to establish a complete data set of system, to include software performance. • Align data to specific test objectives in support of the planned analysis and the overall evaluation.
Evaluation	• Confirm that the tests conducted support the stated test objectives to ensure adequacy of the planned analysis and evaluation. Determine appropriate analysis and evaluation techniques to be incorporated in a system evaluation or a system of systems' evaluation (e.g., STAT, design of experiments, or similar). • Confirm that M&S met test objectives to augment test data and ensure adequacy of evaluation. Identify how accredited M&S (including the validate and verify process) should be used to supplement live test data. • Determine whether the collected data are sufficient to accurately and completely support established measurability metrics. • Determine whether the data collected via M&S tools are sufficient to adequately supplement data collected during live T&E to facilitate a credible evaluation of the system's (or system of systems') realistic survivability and lethality under combat conditions. • Confirm that the collected test data can sufficiently and accurately support the evaluation framework in the approved TEMP or other test strategy documentation. • Relate test results and evaluation conclusions to performance specification and performance results to report on operational significance. • Assess how hardware/software components are brought together to function properly as required in capability documents and what their performance brings to the larger system of systems designed to achieve required capability.
Reporting	• Determine and provide T&E input to all technical and programmatic reviews to support acquisition decision-making. • Assess, document, apply, and/or adapt lessons learned on conduct of test data collection, analysis, and evaluation processes to ensure constant improvement of methods and processes. • Provide the required programmatic T&E reports and/or presentation (quick-look analysis, test reports, analysis reports, software sprint reports, and evaluation reports) to capture test background, methodology,

T&E Phase	T&E Activities
	limitations, results, evaluation, and recommendations to support acquisition decision making and user needs (e.g., development of TTPs, etc). • Archive the data throughout the T&E planning, preparation, T&E execution, analysis, and evaluation phases to support future T&E efforts.

TEST AND EVALUATION CHAPTER 2: URGENT CAPABILITY ACQUISTION

Table of Contents

1. Urgent Capability Acquisition (UCA) Pathway Overview

1.1. Introduction

In accordance with DoDI 5000.02, the DoDI 5000.81 establishes policy and prescribes procedures for acquisition programs that provide capabilities to fulfill urgent operational needs and other quick-reaction capabilities that can be fielded in less than two years. The guidance provided here supports policy established in the DoDI 5000.89 and DoDI 5000.81. In the event of conflict, the reader should defer to policy documentation.

The Executive Director of the Joint Rapid Acquisition Cell (JRAC) assigns responsibilities to the DoD component head for rapid resolution of joint urgent operational needs (JUON), joint emergent operational needs (JEONs), and Warfighter Senior Integration Group (SIG) identified urgent issues. The solution must be capable of being fielded within two years of the validation of the urgent need, in a manner that resolves or substantially mitigates the underlying need. The fielding of an interim solution, even if it provides less-than-full capability, will not be delayed, to enable extended development of immature technology. The estimated cost for any single solution must not exceed $525 million in research, development, and T&E, or $3.065 billion for procurements in FY2020 constant dollars. Urgent capability activities are not necessarily intended to be enduring programs.

The Program Manager (PM) should involve the T&E organizations with the UCA program as soon as the Urgent Operational Need (UON) is identified to support the program decisions and delivery timeline. Contractor testing (CT), government developmental test and evaluation (DT&E), live fire test and evaluation (LFT&E), and operational test and evaluation (OT&E) should be integrated, streamlined, and tailored to the maximum extent practicable to enable efficient use of data and resources across the test program and evaluation of system operational effectiveness, suitability, survivability, and lethality to inform the decision authorities. Test and certification organizations should strive for maximum sharing, reciprocity, availability, and reuse of test results and artifacts. Collaboration between all organizations may lead to the development of digital system models, simulations, and test environments for common use across the spectrum of system test that may produce necessary data or information.

This chapter describes T&E community involvement throughout the UCA pathway lifecycle.

1.2. Urgent Capability Acquisition Pathway Description

The activities for the UCA Pathway, including T&E, are highly tailored to expedite the fielding of capability by streamlining the documentation and reviews normally required as part of the deliberate acquisition process. Figure 1 illustrates the four major phases (often conducted in parallel) within the UCA Pathway: 1) Pre-development, 2) Development, 3) Production and deployment (P&D), and 4) Operations and support (O&S). Details of T&E Community involvement during each phase are discussed in Section 3.

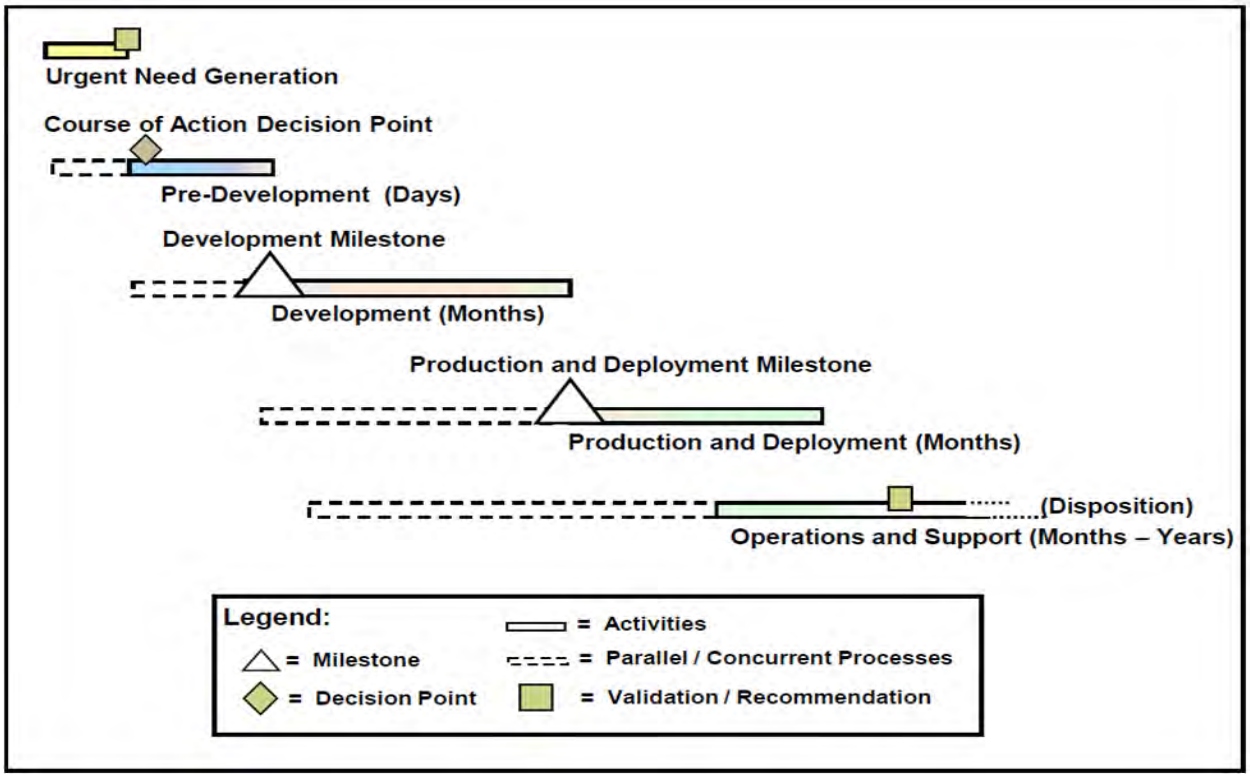


Figure 1. Urgent Capability Acquisition Model[4]

1.2.1. Pre-Development

The purpose of the pre-development phase is to assess and select a course or courses of action to field a quick reaction capability. The PM accomplishes this by developing an Acquisition Strategy. The phase begins upon receipt of either a validated UON, approval of a critical warfighter issue statement by the co-chairs of the Warfighter SIG per DoD Directive 5000.71, or a Secretary of Defense or Deputy Secretary of Defense Rapid Acquisition Authority determination document. During this phase, the Component Acquisition Executive (CAE) appoints a PM and a Milestone Decision Authority (MDA) for JUONs and JEONs assigned to the Component by the Executive Director, JRAC.

The PM identifies a Chief Developmental Tester (CDT) and charters a T&E Working-level Integrated Product Team (WIPT) or equivalent entity responsible for defining the T&E activities and data requirements needed to support the fielding of the urgent capability.[5] The CDT and the T&E WIPT should assist the PM in developing a T&E Strategy, to be documented in the Acquisition Strategy, and later, operational and live fire test plans for assessing how system concepts should be evaluated against operational mission requirements. Government test teams should be involved during this phase to assess the testability of the requirements, if possible, and

[4] 5000.81, December 31, 2019, pg. 10

[5] Different naming convention for the T&E WIPT such as Integrated Test Team are common and acceptable. This document will refer to any of these as the T&E WIPT.

document how testing will be accomplished to adequately demonstrate performance consistent with the UON. Government testers should request that PMs include provisions for sharing possible T&E data sources (e.g., contractor designs and test results, and any artifacts associated with prior testing) in the Request for Proposal (RFP), Statement of Work (SOO), or other contractual material.

Embedding OT&E early in the program helps achieve an efficient test program and should start with OT&E awareness and participation in the pre-development phase. This includes monitoring any contractor or government developmental tests that occur and understanding the pedigree and applicability of the results from developmental testing and any other prior testing that may be usable for operational evaluations. The test community should also identify any gaps in data that will inform test planning for post-deployment assessments.

1.2.2. Development

The MDA approves entry into the development phase. The purpose of the development phase is to evaluate the technical maturity of the preferred solutions and assess any associated risks to performance, safety, suitability, survivability, supportability (including software), and lethality (if appropriate) to determine if the fielding of the capability can be accomplished in the required timelines. The PM will provide the Acquisition Strategy and program baseline, to include the program requirements, schedule, activities, program funding, assessment approach, and intermediate decision points and criteria as the basis for this decision. A tailored T&E Strategy should be included as a part of the Acquisition Strategy. For programs on T&E oversight, operational and live fire test plans should be submitted to DOT&E for approval at this milestone. For programs not on oversight, these documents are approved at the Service level. The role of T&E during this phase is to:

- Assess whether key technologies and subsystems can deliver needed capabilities to reduce the urgent capability gap
- Help ensure that risks (technology, engineering, cyber, integration, safety, etc.) are understood and have been identified, documented, and communicated to the user

Close collaboration with the T&E community during this phase may help to increase the T&E program efficiency.

1.2.3. Production and Deployment

The MDA approves entry into the production and deployment phase. As required, the Services and PMs should conduct OT&E and LFT&E of production-representative systems. The MDA, in consultation with the supporting developmental, operational, and live fire test organizations, and with the concurrence of DOT&E, for programs on T&E oversight, will determine whether the capability has been adequately reviewed, performs satisfactorily, is supportable, and is ready for production and deployment, as well as when assessments of fielded capabilities are required.[6] The MDA will, in consultation with the user and the requirements validation authority, determine which deficiencies must be resolved and what risks can be accepted. The purpose of

[6] DoDI 5000.81, pg. 16

the production and deployment phase is to deliver a system to military units that fills the needed operational capability and satisfies mission needs as informed by the T&E program. For programs on T&E oversight, post-deployment assessment plans should be submitted to DOT&E for approval at this milestone.[7] For programs not on oversight, these documents are approved at the Service level. During this phase:

- The acquiring organization provides the warfighter with the needed capability, to include any required training, spares, technical data, solutions capabilities and limitations, temporary or permanent facilities or infrastructure, support equipment, maintenance, or logistics support necessary for operation
- DoD components coordinate with each other to verify number of items required
- The PM resolves previously identified deficiencies, as necessary

1.2.4. Operations and Sustainment

During the operations and sustainment phase, the PM executes a supportability strategy that meets materiel readiness and operational support performance requirements and sustains the capability in the most cost-effective manner over its anticipated total life cycle. Planning for operations and sustainment phase begins during pre-development and is documented in the Acquisition Strategy. The PM will conduct a post-deployment assessment in coordination with the OTA. No later than one year after the program enters this phase, the DoD component will appoint an official to conduct a disposition analysis which could include termination (demilitarization or disposal), sustainment for current contingency, or transition to a Program of Record.

1.3. Urgent Capability Acquisition Pathway T&E Overview

Figure 2 summarizes the T&E events and associated products as the program progresses through the major phases and milestones of the UCA Pathway. For a UCA, these events and products do not have to happen in sequence but may occur simultaneously to the extent necessary.

[7] DoDI 5000.81, pg. 17

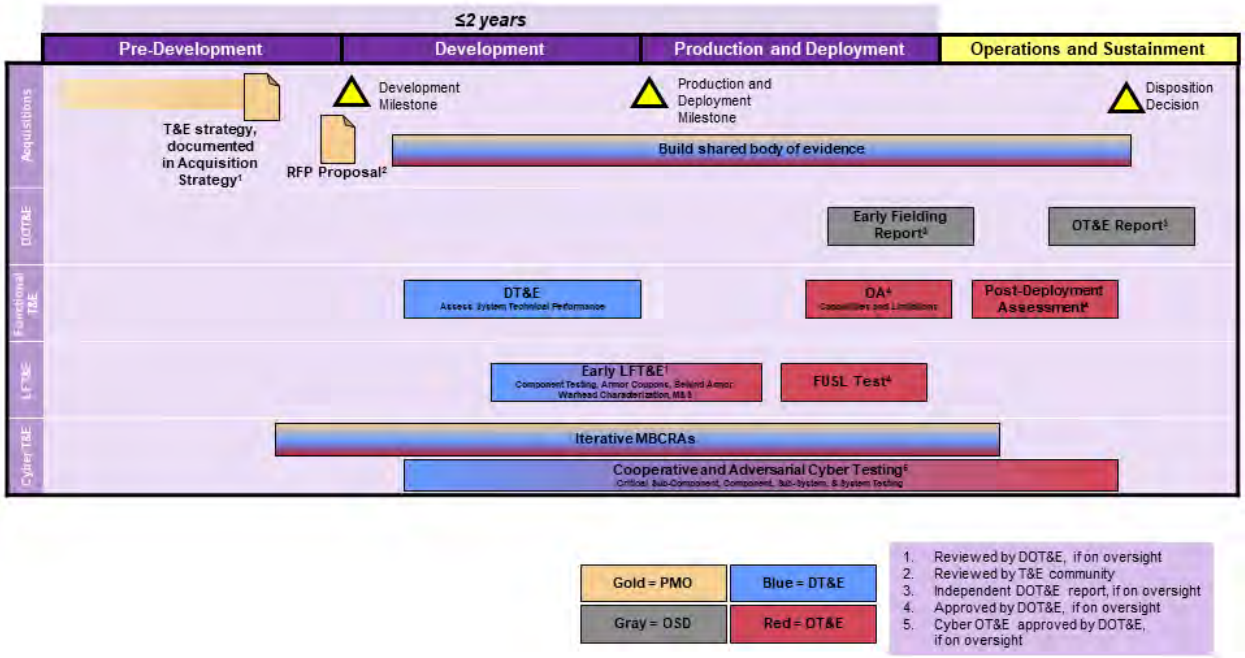


Figure 2. T&E Aligned with UCA Pathway

Test and Evaluation Working-level Integrated Product Team (WIPT)

The T&E WIPT should coordinate top-level planning for all products and test events shown in Figure 2 and the integrated schedule. The T&E WIPT defines the data requirements and T&E resources needed to adequately plan and execute the T&E program. The PM, in coordination with the T&E WIPT, should ensure the T&E requirements are included in RFPs and then the acquisition contract to support the availability and access to data needed to mitigate risk to the T&E program. In addition to contracts, when appropriate, the T&E WIPT should participate in acquisition program requirements refinement to ensure their measurability, testability, achievability, and relevancy to the operational mission. The T&E WIPT may request clarity from the requirements authority for any requirements found untestable.

The T&E WIPT includes representatives from all organizations responsible for providing or overseeing the T&E program development and its execution. In particular, the T&E WIPT should include representatives of test data stakeholders such as systems engineering, DT&E, OT&E, LFT&E, the user, product support, the Intelligence Community, and applicable certification authorities. The T&E WIPT should enable collaboration among stakeholders to maximize efficiency by planning and executing an integrated T&E program that leverages all test events for the purposes of meeting developmental, live fire, and operational evaluation objectives. The PM should ensure that results from all test events are captured in a shared data repository and available for all parties to use for independent assessment.

- Government test teams should strive to maintain a tempo for testing that supports the required decisions using various tools (e.g., digital engineering, sequential testing, automation).
- Government test teams should develop a tailored T&E program consistent with filling the urgent need with end-to-end mission threads and actual users.

- OT&E and LFT&E should concentrate on appropriately scoped, dedicated tests while integrating usable data and information that meet stakeholder needs, support operational evaluations, and inform decisions
- T&E WIPT should develop collaborative test data scoring to evaluate available test data for potential, to include in any OT&E and LFT&E assessments

2. Test and Evaluation Planning for Urgent Capability Acquisition Pathway

The purpose of T&E planning is to develop an approach to credibly demonstrate the extent to which the technical, functional, and operational capability meets the urgent need. As the planning process is critical and sets the conditions for success, all test teams should be involved early in the program to establish and document how testing and modeling and simulation (M&S) will support the analysis and evaluation of the system performance. The T&E WIPT should identify the measures to be used to evaluate the system as a part of the planning process, and then the data needed and conditions under which those data will be collected.

T&E planning should be digitized and automated as much as possible to support continuous development, integration, and delivery of system capabilities. Digital test management tools automate the process of test planning, scheduling, tracking, and reporting test events.

During the planning process, various stakeholders are developing documentation, summarized and defined in Table 1, to include the associated testing resources, tools, and infrastructure. This section explains the role of T&E in this process.

Table 1. Planning Documents

Artifact	Description	Developed by
Requirements Document	Specifies the validated operational requirements for the system to deliver the capability that meets operational performance criteria. Documents the need for a materiel approach to close a specific capability gap.	Sponsor
Acquisition Strategy, including T&E Strategy	Contains only essential information such as resourcing needs and sources, key deliverables, performance parameters, key risks and mitigation approaches, a production schedule and fielding schedule; contracting methodology and key terms; and preliminary plans for performance assessment of the capability and its supportability, to include software.	Program Manager with support from T&E WIPT
Request for Proposals	A document used in negotiated acquisitions to communicate government requirements, including those for T&E, to prospective contractors and to solicit proposals.	Program Manager
Tailored Test Plans	Defines the processes by which technical, functional, and operational performance will be tested and evaluated to satisfy developmental test and evaluation criteria, and to demonstrate operational effectiveness, suitability, survivability, and lethality.	T&E WIPT

2.1. T&E Content and Interests in Planning Documents

The success of T&E relies heavily on each of the documents outlined in Table 1. The T&E community should work with the acquisition community on these documents, especially the

acquisition strategy, to incorporate needed T&E information. This section highlights T&E content and involvement of test teams in the development of each of these documents.

2.1.1. Requirements Document

The T&E WIPT should be involved with the requirements documentation early, and determine whether the capability requirements from the UONs/JUONs/JEONs documents are defined sufficiently to assess testability and are relevant to the operational mission. The T&E WIPT should, if possible, ensure the clarity and measurability of requirements, that the measurements to establish technical feasibility are incorporated, and that requirements traceability exists from the capability-level requirements to the test events. These requirements may be further informed by supporting information found in the Validated Online Lifecycle Threat Report (VOLT) or theater intelligence assessments. Test teams should:

- Understand what constitutes the required mission effectiveness, suitability, survivability, and lethality and how that will be measured
- Determine whether cyber and interoperability needs are clearly defined in the requirements document

2.1.2. Acquisition Strategy

The Acquisition Strategy includes a tailored T&E Strategy, production and fielding schedule, contracting methodology and key terms, and an initial concept for operations and support, including support funding. To support the development of the Acquisition Strategy, the T&E community should collaborate on a tailored T&E Strategy with the PM. Early coordination of the strategy with the developmental, operational, and live fire test organizations is crucial to a streamlined process. The Acquisition Strategy should describe the development and decisions sufficiently to convey what information/data testing needs to provide, and when to adequately support the acquisition decisions and evaluate the technical, functional, and operational performance. The Acquisition Strategy should account for T&E when identifying resource needs. Test teams should:

- Ensure that T&E requirements and data delivery for the contractor are described at a high level and included with more detail in the RFP
- Ensure that time is allotted in the program schedule for independent government T&E
- Ensure that the Acquisition Strategy addresses a robust T&E program, to include a cyber T&E program
- Describe how data will be accumulated to build a shared body of evidence
- Include a tailored integrated decision support key (IDSK) that outlines the acquisition, technical, and program decisions and the data (e.g., CT, DT, LFT, OT, M&S) necessary to support those decisions (the IDSK may produce efficiencies across the T&E lifecycle by integrating DT, CT, and OT)

Early briefings of the T&E Strategy contained in the Acquisition Strategy by the Program Office and the OTA to Service stakeholders, the Under Secretary of Defense for Research and Engineering (USD(R&E)), and DOT&E for programs on the T&E Oversight List are required to

facilitate cross-organizational alignment and subsequent approval of operational and live fire test plans.

2.1.3. Request for Proposals (RFP)

The RFP defines what the government expects from the contractor. T&E expectations should be stated in the RFP and the acquisition contract. The Acquisition Strategy is a source document for the RFP and should be generated in time to support RFP development. The PM should consult with government test teams to ensure that the RFP supports data collection for government T&E. The test teams should ensure that the following items and activities are included as contract deliverables:

- Government access to contractor test events, test tools, test data repositories, and test environments
- Delivery of contractor-provided M&S tools to be used by government test organizations; these may include initial digital system models, component level reliability and availability models, or other M&S tools
- Contractor test plans, procedures, reports, and data
- Contractor support for government testing, including early live fire testing

2.1.4. Tailored Test Plans

2.1.4.1. Developmental Test Plans

For a UCA program, key elements of DT test planning are the tailoring of the plan and the synchronization of parallel test activities that support the urgency of the pathway. The key elements to be addressed are:

- Confirming the needed development and availability of existing technologies
- Characterizing performance, safety, suitability, survivability (including cybersecurity), supportability (including software), and lethality (if required), to support the MDA's production decision
- Supporting T&E, as appropriate, to facilitate transition to an enduring capability
- Maximum integrated T&E to the extent possible, to include cyber T&E to share data and resources

In general, this will involve increased embedding of T&E personnel on the development team to both tailor the activities and ensure the key elements are addressed.

2.1.4.2. Operational and Live Fire Test Plans

The T&E WIPT should ensure the operational and live fire test plans are tailored, streamlined, feasible, and support the UCA timeline and Acquisition Strategy. These plans serve as an agreement between the PM and the T&E stakeholders for T&E resources, and roles and responsibilities. The plans should capture the data requirements and processes by which the system will be tested and evaluated to enable the evaluation of the missions the system is intended to perform while considering relevant interfacing systems, threats, and operational environments. For a UCA program, test plans should focus the collection and analysis of data on only those T&E activities directly related to the theater of employment, mission context (types of

operations, threats, environments, users, and tactical employment), and technical requirements identified in the Urgent Operational Needs. Testing should include collaboration among all relevant stakeholders.

The T&E WIPT should ensure the operational and live fire test plans are executable and align with the T&E Strategy as defined in the Acquisition Strategy, T&E policy (DoDI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. The operational and live fire test plans should define the conditions under which required data will be collected, and any tools required to manage the data and perform the testing. OT should consider informing the DT community of their OT data requirements and plans to meet their evaluation objectives, and vice versa. As such, DT should consider the operational relevance of the developmental tests to identify operationally representative deficiencies.

The Services will develop the LFT&E strategy that identifies the data elements and test events required to evaluate the survivability and/or lethality of a system. For programs under T&E oversight, operational and live fire test plans will be submitted to DOT&E for approval at the Development Milestone; post-deployment assessment plans will be submitted to DOT&E for approval at the Production and Deployment Milestone. DOT&E will ensure that testing is rigorous enough to rapidly evaluate critical operational issues. Test plans submitted for DOT&E approval are required to be delivered 60 days before the start of testing. For programs on OSD T&E oversight, DOT&E is the final approver for the operational and live fire test plans.[8]

2.1.5. Full-Up System-Level (FUSL) Waiver Process

Programs that intend to field urgent capabilities must still meet the requirements of 10 U.S.C. §§ 4172 to conduct "realistic survivability testing" or "realistic lethality testing" before proceeding to a fielding decision. The term "realistic survivability testing" means testing for vulnerability of the system in combat by firing munitions likely to be encountered in combat (or munitions with similar capabilities) at the system configured for combat. The DoD normally considers FUSL testing that meets the requirements of 10 U.S.C. §§ 4172 unless a waiver from FUSL is granted by DOT&E. Likewise, the term "realistic lethality testing" means firing production-representative munitions or missiles at targets, or classes of targets, under conditions sufficiently realistic to demonstrate the lethality effects the weapon is designed to produce. This is commonly referred to as end-to-end testing.

The Live Fire Test Law contains provisions for a waiver from the requirement for FUSL testing. The law states that any waiver must be approved as soon as is practicable after program initiation depending on the specifics of the acquisition schedule for a given system. The waiver package sent to Congress consists of two parts: certification that the waiver is needed (on the basis of both cost and practicality), and an alternative LFT&E plan for evaluating survivability or lethality. These two parts require coordination between the acquisition executive and DOT&E. Technically, there is no waiver from LFT&E, only from the requirement for FUSL or end-to-end testing.

The Live Fire Test Law requires that the alternative LFT&E plan has a basis in testing. Paragraph (c)(2) states that "the Secretary may waive the application of the survivability and

lethality tests…and instead allow testing of the system or program in combat by firing munitions likely to be encountered in combat at components, subsystems, and subassemblies…" Thus, the alternative LFT&E cannot be based solely on M&S and other kinds of analyses. The law names the following as potential data sources in addition to testing: design analyses, M&S, and analysis of combat data.

The Live Fire Test Law states, "At the conclusion of survivability or lethality testing, the Secretary of Defense shall submit a report on the testing to the congressional defense committees. Each report shall describe the results of the survivability or lethality testing and shall give the Secretary's overall assessment of the testing." Per DoD Directive 5141.02, the Secretary of Defense has delegated this responsibility to DOT&E.

2.2. T&E Resources

The operational and live fire test plans should document the T&E resources required to support DT&E, OT&E, and LFT&E. Programs should identify one-of-a-kind T&E resources and long-lead items early in the acquisition process, if they are necessary, to allocate adequate funding for development and use. The PM should coordinate with the T&E stakeholders for all test infrastructure and tools (e.g., models, simulations, automated tools, synthetic environments) that support acquisition decisions to be verified and validated, if possible, by the intended user or appropriate agency.

These resources include, but are not limited to:

2.2.1 Test articles (e.g., the system under test, test targets and expendables, threats)

The environments used to conduct testing for OT&E should represent the operationally realistic environment as closely as possible, including threats and realistic system use. This requires the interfacing systems that form the system of systems with the program of record.

2.2.2. Test facilities, infrastructure, instrumentation and ranges, to include cyber ranges and test team, software integration laboratories

Programs should use government T&E capabilities unless an exception can be justified as cost-effective to the government. PMs should conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the operational or live fire test plan approval process before acquiring or using non-government test facilities or resources.

The test plans should also include any proposed use or application of embedded instrumentation, including for use to gather post-deployment data. The intent of embedded instrumentation is to facilitate data collection and system diagnostics without modifying the system's operational configuration. The PM should work with the T&E WIPT and other stakeholders to plan for the use of embedded instrumentation to collect system performance and diagnostic data whenever feasible, and should document a plan to obtain independent accreditation and certification in the operational or live fire test plans prior to use in assessments, if possible. This may include adding requirements for these embedded instrumentation in program RFPs, and other resourcing provisions.

2.2.3. Automated testing tools

Automated test execution tools may be part of the process of executing test cases or procedures on the system under test. The T&E WIPT and PM should work with the contractor to understand the contractor's tools, specifically their verification and validation plans, and the credibility of those tools for the intended use. It is encouraged for government test teams to be trained with these tools so they can use their outputs to inform evaluations. Such expectations should be clarified in the appropriate contractual provisions. In some cases, government test teams may become experts in the tools used by both the contractor and government. The automated tools should also provide visibility into any continuous testing so that stakeholders can gain confidence on the quality of the data received.

2.2.4. M&S, and their verification and validation plans

The test plans should document any planned M&S with the strategy and schedule, including the using organization, intended use, and the commitment to provide a verification and validation plan for each tool or test infrastructure asset. The PM should coordinate with the T&E WIPT to ensure the program RFPs include a requirement to deliver system M&S tools for use by government test organizations, if available. These may include initial digital system models, component level reliability and availability models, or other M&S tools.

2.2.5. Manpower and personnel

The test plans should include information about friendly and threat operational forces, data collectors, and subject matter experts that will be required to execute the T&E program.

2.2.6. Federal/State/local requirements, range requirements, and any special requirements

This may include requirements for explosive ordnance disposal, corrosion prevention and control, or frequency management and control.

2.2.7. Shared Body of Evidence and Data Repository

During the Pre-Development Phase, the PM should establish a shared data repository to store data and provide access to all test teams so that they can review, use, and input these test data to meet their objectives. This should enable the use of sequential testing, big data analytics, and other adaptive methods in support of T&E efficiencies. Throughout system development, T&E should be building a shared body of test evidence to support efficient technical, functional, and operational performance evaluations and adaptive T&E. Relevant test data gathered through all testing should be included in this test data repository. To enable adequate use of sequential testing and similar T&E planning and analysis methods, the T&E WIPT may leverage existing or develop collaborative test data scoring boards to evaluate integrated test data for potential to meet OT&E or LFT&E requirements. The OTA should maintain the authoritative record for these test data that meet OT&E or LFT&E requirements and will be considered in the operational evaluation.

2.2.8. Projected and actual level of funding

T&E funding in the resources section should be consistent with the cost estimate and budget submissions.

3. T&E During Urgent Capability Acquisition Pathway Phases

3.1. Pre-Development Phase

Specific T&E activities within the Pre-Development Phase include:

- Coordinate the T&E Strategy
- Actively participate in the development of the requirements and RFPs, as appropriate
- Inform the Development Milestone Decision

3.1.1. Coordinate the T&E Strategy

In coordination with the PM, the T&E WIPT should develop the T&E Strategy before progressing to the Development Phase. The T&E Strategy should plan for the major resources required for adequate T&E in accordance with the requirements, intended use of the system, and given the operationally relevant threat as outlined in the VOLT. The T&E Strategy should document any risks and describe how the PM will mitigate these risks. Documentation should be tailored, included in the Acquisition Strategy and relevant developmental, operational and live fire test plans, and consider:

- An integrated program schedule aligning T&E events and reporting requirements to the broader Acquisition Strategy and accounting for report generation timelines
- A tailored IDSK that links DT&E, OT&E, and LFT&E information to critical decisions
- Evaluation focus areas for DT&E, OT&E, and LFT&E
- Evaluation frameworks that present the overarching approach to DT&E, OT&E, and LFT&E, and identify opportunities for integrated testing
- Brief descriptions and objectives of individual test phases and events, and test limitations or constraints that could degrade or prevent evaluations tied to the operational need, safety, or mission capability
- Resources and test support requirements needed for all test phases and events, and funding sources for all test resources

3.1.2. Inform the Development Decision

The MDA approves the Acquisition Strategy, including the T&E Strategy, to inform the Development Milestone Decision. The PM provides the Acquisition Strategy and program baseline, to include the program requirements, schedule, program funding, assessment approach, test strategy, and intermediate decision points and criteria. The MDA reviews the information to determine that the capability can be fielded within two years, does not require substantial developmental effort, is based on proven and available technologies, and identifies any exceptions to these preferred conditions. The MDA approves the tailored acquisition baseline and testing approach, and initial quantities to be produced and assessed (DoDI 5000.81, December 31, 2019, Section 4.3). At the development milestone, if the system is on T&E oversight, the operational and live fire test plans should also be provided to DOT&E for approval.

3.2. Development Phase

Major T&E activities in the development phase include:

- Review the Logistics Risk Assessment
- Conduct government T&E, to include developmental tests in collaboration with Operational Test Agencies and LFT&E to:
    - Demonstrate that preferred technology is feasible, affordable, supportable, and satisfies requirements in a mission context, to the maximum extent possible
    - Confirm maturity, as needed, of technologies identified by the MDA at entry into development
    - Gain user feedback by integrating operational users as soon as possible
    - Conduct cyber testing
    - Obtain authorization for IT systems in accordance with DoDI 8510.01, Risk Management Framework for DoD Information Technology
- Coordinate VV&A plans, if necessary
- Coordinate operational and live fire test plans, including the OA
- Inform the Production and Decision point

3.2.1. Review the Logistics Risk Assessment

A logistics risk assessment is an analysis of a program's product support strategy across the system lifecycle, including sustainment costs. During this phase, the PM, supported by the T&E community (and when practical, an independent and impartial team of Subject Matter Experts) should conduct an abbreviated logistics risk assessment as part of life cycle considerations. The PM finalizes sustainment requirements and decomposes sustainment requirements for use during the logistics risk assessment.

3.2.2. Conduct Government T&E

Developmental T&E. Government testers should continue to leverage contractor-conducted DT&E when appropriate to supplement government DT&E. Involving users in government-conducted DT&E also encourages integrated T&E activities by increasing the relevance of the data to the OT&E stakeholders. The OTAs should participate in the planning and execution of developmental T&E to adequately leverage the data and inform the operational T&E.

DT&E activities should be streamlined and focused on assessing the technical performance of the system to reduce the capability gap. Initially, this focuses on reducing uncertainty and risk concerning the maturity and availability of components and technologies planned for the system. Much of this will be testing at the component level, yet it is still essential that this be done in a mission-informed context. That is, components should be tested under the technically stressing conditions likely to be imposed by operations. Similarly, system-level developmental testing, when possible, should be conducted in an environment similar to the one in which the system will be employed, and in a mission-oriented context using service members from the user community who will operate the system once fielded. This should include testing the system in its expected cyber-contested environment. Early integration of both component and system

testing in this fashion are essential because of the compressed acquisition timeline. The early integration of operational users should be resourced-for in the Acquisition Strategy.

Early integration of operational considerations and, where possible, operational users in T&E activities, is critical in reducing the amount of time required to find and fix system/performance deficiencies and safety concerns and then retest, capturing immediate feedback and recommendations from the user, and reducing overall program risk. Additionally, multiple and iterative T&E events may be necessary to ensure the user and developer can substantiate that a proposed solution is feasible and supportable, satisfies validated urgent capability requirements, and identifies and mitigates operational and accidental risk factors.

Representatives from the operational and developmental T&E community should be fully embedded and participate in these events, with access to all records and data to ensure shared understanding of test results, as well as reduce the amount of time required for dissemination of information and data. The T&E WIPT should codify responsibilities and data-sharing obligations as well as implement program protection measures to prevent disclosure of critical information.

Live Fire Test and Evaluation. LFT&E generates information that supports the evaluation of a system's operational effectiveness, suitability, survivability and lethality. The DOT&E approves LFT&E test plans (including survivability and lethality test plans) for covered systems as defined in 10 U.S.C. §§ 4172. DOT&E also approves the quantity of test articles procured for all LFT&E test events for any system under LFT&E oversight. During this phase, LFT&E activities should be narrowly scoped and focused on the new capability defined in the UONS, and the threats likely to be encountered. Testing may include testing of components and subsystem as well as early M&S assessments of survivability or lethality to provide a baseline from which system improvements to survivability or lethality can be made or measured.

3.2.3. Inform the Production and Deployment Decision

At the Production and Deployment milestone, the PM informs the MDA of the results of development activities, pre-deployment performance, and the program assessment to-date. The PM will present plans to transport, deploy, and sustain the capability, conduct post-deployment assessments, and train maintenance and operating personnel to the MDA for approval. The MDA, in consultation with the supporting developmental and operational and/or live fire test organization, and with input from DOT&E for programs under DOT&E oversight, will determine:

- Whether the capability has been adequately reviewed, meets the desired capabilities in the UONS, performs satisfactorily, is supportable, and is ready for production and deployment
- When assessments of fielded capabilities are required

Using the provided information, the MDA decides whether to produce and, in coordination with the requester/user, field the capability, approves the updated Acquisition Strategy, and documents the production decision in an Acquisition Decision Memorandum (ADM). MDAs may authorize production at the same time development is approved.

3.3. Production and Deployment Phase

Major T&E activities within the Production and Deployment phase may include:

- Testing the mitigation of critical deficiencies
- Update VV&A plans, if necessary
- Coordinate post-deployment assessment plans
- Complete Government T&E Testing, to include the Operational Assessment (with a cybersecurity assessment) and LFT&E (to include FUSL) informed by the most recent intelligence, threat, and concept of operations/operational mode summary/mission profile documents for changes that may affect the validity of the characterization
- Deliver the OA and LFT&E reports

3.3.1. Complete Government T&E

Operational Test and Evaluation. The Service OTA conducts the Operational Assessment (OA) in accordance with an approved test plan. OAs include trained military users employing the system in operationally representative conditions, in a mission-ready system configuration against representative threats. Because of the accelerated timeline, OA execution will likely differ from other acquisition pathways in the following ways:

- Testing may occur simultaneously in overlapping phases (Development and Production and Deployment)
- Testing focuses on the necessary testing for the specific theater of employment, anticipated threats, and mission set to meet the urgent operational need
- First unit equipped is the test unit

For programs on T&E oversight for operational and live fire testing, after test completion, DOT&E will produce an OA report.

Live Fire Test and Evaluation. The Production and Deployment Phase of LFT&E typically includes system-level and FUSL tests, unless a waiver from FUSL has been approved. Live Fire Testing and M&S are used to support an evaluation of the survivability in a contested environment, to include susceptibility to attack, vulnerability to a hit, the effect(s) of those vulnerabilities on residual mission capability and crew casualties, and recoverability from the hit.

Because of the UCA accelerated timeline, LFT&E execution will likely differ from other acquisition pathways in the following ways:

- Testing may occur simultaneously in overlapping phases (Development and Production and Deployment)
- Testing focuses on the necessary testing for the specific theater of employment and mission set to meet the urgent operational need
- Waiver of FUSL or end-to-end testing may allow production and deployment of systems to occur prior to completion of LFT&E

3.3.2. Deliver OA and LFT&E Reports

At decision points identified in the acquisition strategies, a report will be provided to the decision maker. For interim assessments, the report should document the status of the system's capability to meet operational effectiveness, suitability, survivability, and lethality requirements. The report should also highlight observed capabilities and deficiencies. If the system proceeds to operational use at this stage, DOT&E will provide an Early Fielding Report, which will report on whether the T&E results confirm that the system is operationally effective, suitable, survivable, and lethal, if applicable. Reports will be required by the Service from both the lead developmental test organization and the OTA. For programs on T&E oversight, DOT&E will submit an independent OA (typically an Early Fielding Report) and live fire reports to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition and Sustainment, congressional defense committees, and Military Service secretaries, as well as the Service acquisition executives. The Service OTA provides an independent report assessing the capabilities and limitations of the required system to meet the urgent operational need. For T&E oversight programs, the Service OTA provides the report to DOT&E (DoDI 5000.89, November 19, 2020 Section 6.4.c).

3.4. Operations and Support Phase

Planning for O&S begins during pre-development and is documented in the Acquisition Strategy. Major T&E activities within the O&S phase may include:

- Post-deployment assessment
- Capability improvements
- Disposition analysis

3.4.1. Post-Deployment Assessment

A post-deployment assessment should be conducted by the OTA after deployment. If practical, the OTA will conduct the assessment in the field using representatives from the supporting operational test organization. If not, the OTA may use alternate means such as surveys to collect user feedback or other DoD component feedback. DOT&E will independently review and approve all post-deployment assessment approaches for all programs under T&E oversight for operational and live fire testing following submission at the Production and Deployment milestone. For programs not on T&E oversight, these plans should be approved at the Service level.[9]

[9] 5000.81, pg. 13

3.4.2. Capability Improvements

The PM or user community may propose urgently needed capability improvements to address deficiencies identified during the OA. If the recommended improvements fall within the scope of the initial requirement, the procedures stated in DoDI 5000.81 may be used by the PM to acquire the improvement. If the recommended improvement falls outside the scope of the initial requirement, a new or amended requirement document from the PM may be needed. For programs on DOT&E oversight, a test plan may be required.

3.4.3. Disposition Analysis

Post-deployment arrangements are known as the disposition of the capability. The disposition analysis considers the performance of the fielded capability, mishap data, long-term operational needs, and the relationship of the capability to the component's current and planned inventory of equipment. The analysis will also consider the continuation of non-materiel initiatives, the extension of science and technology developments related to the fielded capability, and the completion of MDA-approved and funded materiel improvements. Based on the analysis, a disposition official, appointed by the DoD component, will recommend that the capability be demilitarized and disposed of, will continue for the current contingency, or serves an enduring purpose and may be transitioned to a program of record.

TEST AND EVALUATION CHAPTER 3: MIDDLE TIER OF ACQUISITION

Table of Contents

1. Middle Tier of Acquisition (MTA) Overview

1.1 Introduction

In accordance with DoDI 5000.02, the DoDI 5000.80 establishes policy and prescribes procedures for the management of the MTA for rapid prototyping and rapid fielding in Section 804 of Public Law 114-92. The guidance provided here supports policy established in the DoDI 5000.89 and DoDI 5000.85. In the event of conflict, the reader should defer to policy documentation.

The MTA Pathway is intended to fill a gap in the defense acquisition system for those capabilities with a level of maturity to allow them to be rapidly prototyped or fielded, within five years of MTA program start. The intent for programs using the pathway is to accelerate capability maturation before transitioning to another acquisition pathway, or to minimally develop a capability before rapidly fielding. Technology sources for MTA pathways include available or emerging commercial technology, maturing technology from government labs, Defense Prime Independent Research and Development (IR&D) efforts, and innovative Small Business Innovation Research (SBIR) solutions. Major systems intended to satisfy a major interagency requirement primarily focus on technology development or have significant international partner involvement are discouraged from using the MTA pathway. Table 1 provides an overview of each MTA pathway, to include key differences and characteristics.

Table 1. Comparison of Middle Tier Acquisition Pathway

	Rapid Prototyping	Rapid Fielding
Purpose	• Based on innovative technology • Rapidly develops fieldable prototype • Produces a new capability • Meets emerging military needs	• Based on proven technology • Delivers field production quantities of new or upgraded systems • Requires minimal development
Objective	• Field prototypes meeting defined requirements that can be demonstrated in an operational environment • Can provide for residual operational capability within five years from MTA program start date	• Field proven technologies with minimal development • Initiate production within six months and complete fielding within five years from MTA program start date

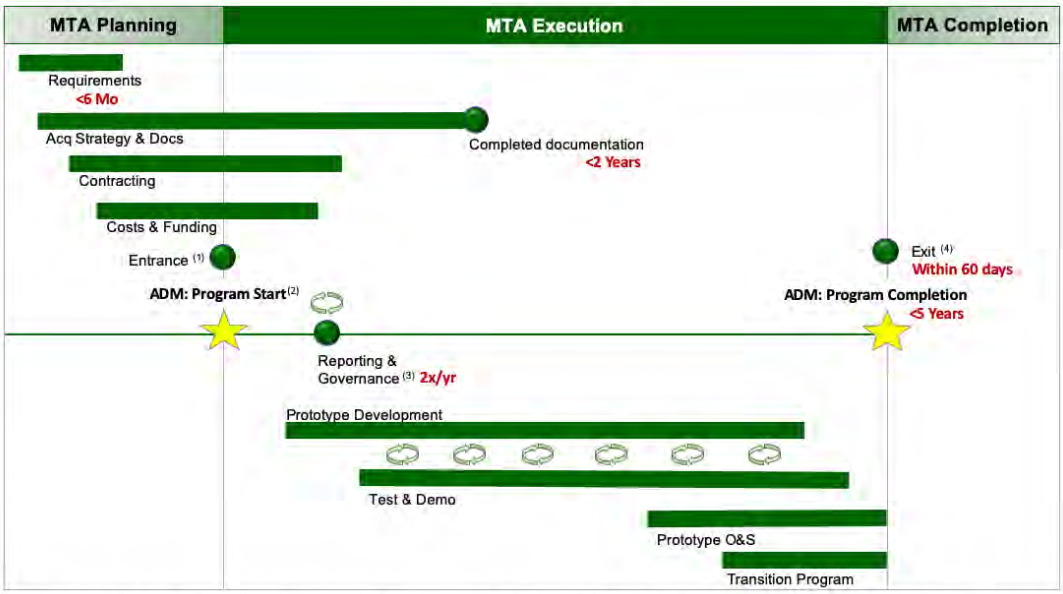
The Program Manager (PM) should involve the T&E organizations with the acquisition program from its inception and throughout its lifecycle to support the program decisions and delivery timeline. Contractor testing (CT), government developmental test and evaluation (DT&E), live fire test and evaluation (LFT&E), and operational test and evaluation (OT&E) should be integrated, streamlined, and automated to the maximum extent practicable to enable efficient use of data and resources across the test program and evaluation of system operational effectiveness, suitability, survivability, and lethality to inform the decision authorities. Maximum sharing, reciprocity, availability, and reuse of test results and artifacts among testing and certification organizations are encouraged for success. Collaboration between all organizations should be considered to develop digital system models, simulations, and test environments for common use across the spectrum of system tests that may produce necessary data or information.

This chapter describes T&E community involvement throughout the rapid prototyping and rapid fielding pathways.

1.2 Middle Tier of Acquisition (MTA) Pathway Description

1.2.1 Rapid Prototyping

The purpose of the rapid prototyping pathway (shown in Figure 1) is to provide for the use of innovative technologies to rapidly develop fieldable prototypes, demonstrate new capabilities, and meet emerging military needs. Rapid prototyping efforts are intended to determine whether a new technology or application of technology provides improved mission capabilities. The objective is to field a prototype that meets defined requirements that can be demonstrated in an operational environment and provide for a residual operational capability within five years of the MTA program start date.



(1) *Major Systems*: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

Figure 1. Middle Tier of Acquisition Rapid Prototyping Pathway Model[10]

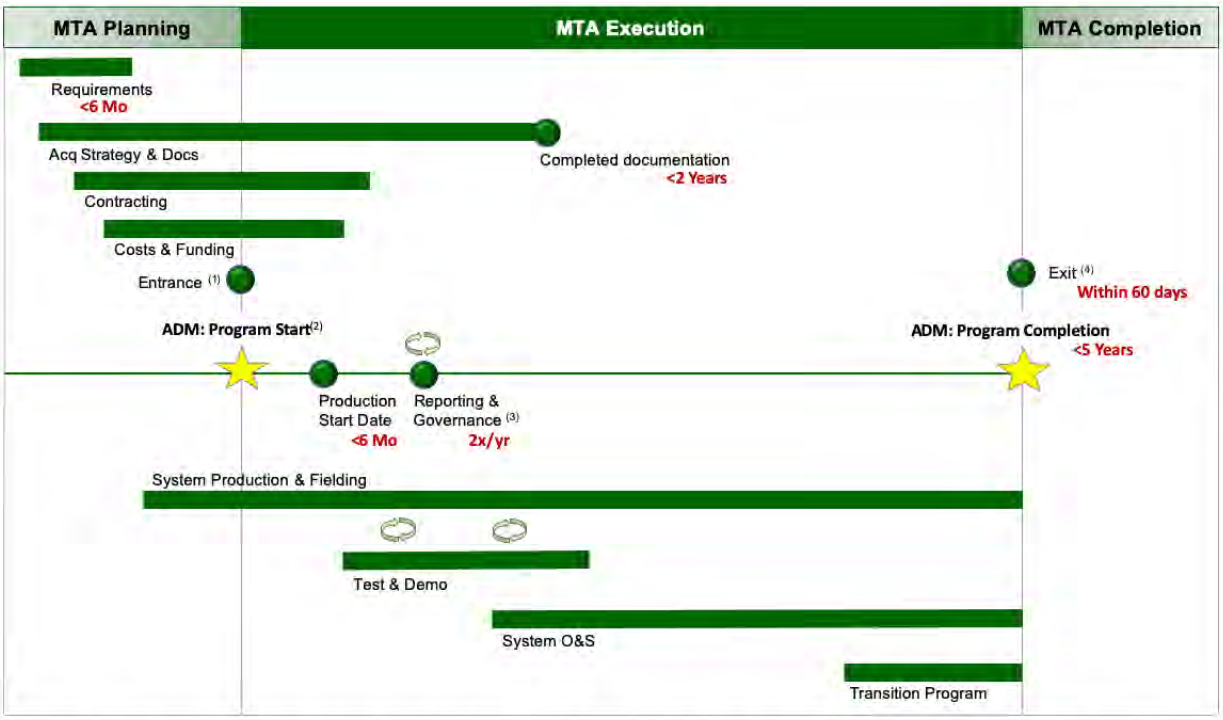
DoD Components will develop a merit-based process for the consideration of innovative technologies and new capabilities to meet needs communicated by the Joint Chiefs of Staff and the Combatant Commanders. DoD Components will develop the process to implement acquisition and full funding strategies for the program. This process will result in an Acquisition Strategy, which includes security, schedule, and production risks, and a cost estimate. DoD Components will develop a process for demonstrating performance and evaluating for current operational purposes the proposed products and technologies, and should document this process in the T&E Strategy. For each MTA program, DoD Components will develop a process for

[10] DAU website.

transitioning successful prototypes to new or existing acquisition programs under the rapid fielding pathway or other acquisition pathway. This process will result in a transition plan, included in the Acquisition Strategy, which provides a timeline for completion within two years of all necessary documentation required for transition, after MTA program start.[11]

1.2.2 Rapid Fielding

The purpose of the rapid fielding pathway (shown in Figure 2) is to provide for the use of proven technologies to field production quantities of new or upgraded systems with minimal development. The objective is to begin production within six months and complete fielding within five years of the MTA start date.



(1) Major Systems: Acquisition Decision Memorandum(ADM) signed by the Decision Authority (DA), Acquisition Strategy (which includes [1] Security, Schedule & Production Risks; [2] Test Strategy/Results; and [3] Transition Plan), and Program Identification Data (PID)
Non-Major Systems: ADM signed by the DA, PID
(2) Major Defense Acquisition Programs (MDAPs) require Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) Prior Written Approval
(3) Updated PID submitted twice a year with President's Budget and Program Objective Memorandum submissions to Office of Secretary of Defense (OSD)
(4) Signed Outcome ADM, Final PID, Assessment of Test Results

Figure 2. Middle Tier of Acquisition Rapid Fielding Pathway Model[12]

DoD Components will develop a merit-based process for the consideration of existing products and proven technologies to meet needs communicated by the Joint Chiefs of Staff and the Combatant Commanders. DoD Components will develop the process for demonstrating operational performance and evaluating for current operational purposes the proposed products and technologies. This process should be documented in a T&E strategy. DoD Components will develop and implement acquisition and full funding strategies for the program, as well as a

[11] DoDI 5000.80, pg. 8

[12] DAU website.

process for considering lifecycle costs and address issues of logistics support and training; system, joint, and coalition interoperability; and planning for cooperative opportunities, to include foreign sales. For each MTA program, DoD Components will develop a process for transitioning successful programs to operations and sustainment. This process will result in a transition plan, included in the Acquisition Strategy, which provides a timeline for completion within two years of all necessary documentation required for transition after MTA program start.[13]

2. Middle Tier Acquisition Pathway T&E Overview

The T&E community plays a critical role in collecting and analyzing test data and information to assist the Decision Authority (DA) in managing risks and making informed outcome determinations and transition decisions. A T&E program for an MTA should consider the Acquisition Strategy, user requirements, and outline cost and resource estimates needed to accomplish its goals within the directed timelines. Figure 3 summarizes the T&E events and associated products for the rapid prototyping and rapid fielding MTA pathways.

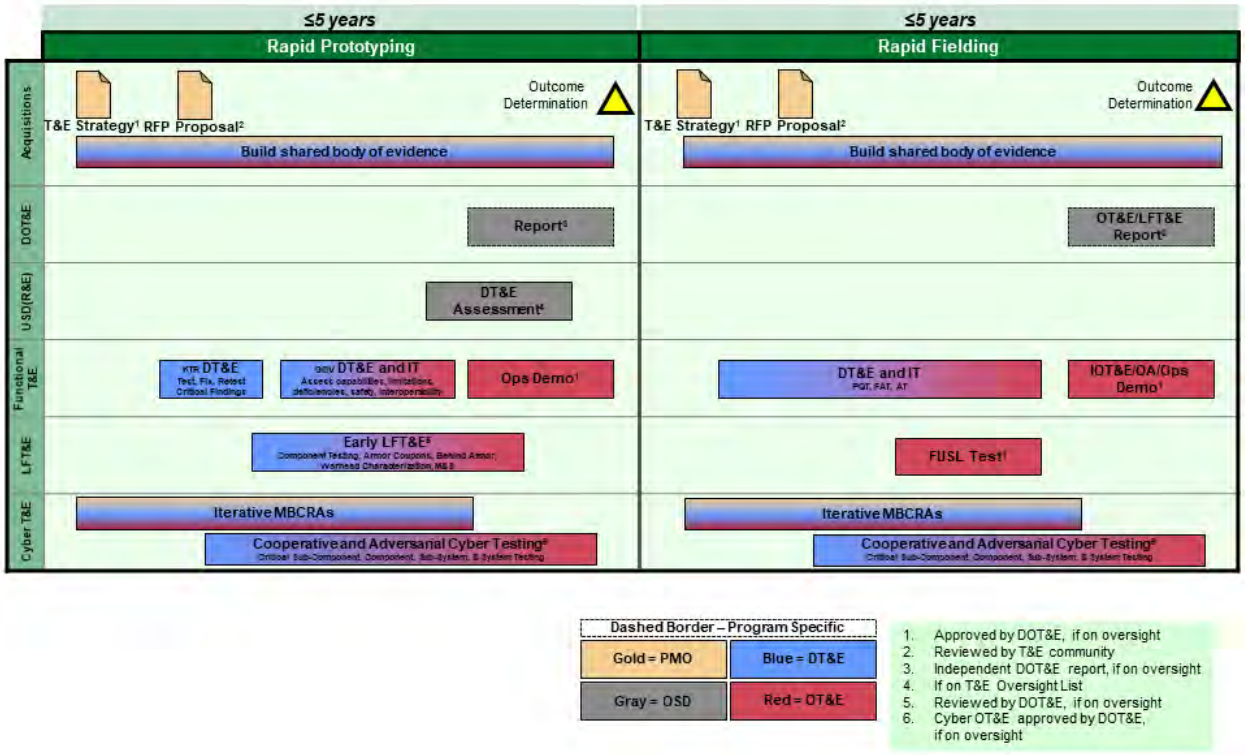


Figure 3. T&E Aligned with MTA Pathway

[13] DoDI 5000.80, pg. 8-9

2.1 Test and Evaluation Working-level Integrated Product Team (T&E WIPT)

During the MTA planning phase, the PM should charter a T&E WIPT or equivalent entity responsible for defining the T&E activities and requirements.[14] The T&E WIPT coordinates top-level planning for all test events and documents listed in Figure 3 and the schedule, which should account for the time needed to fix any deficiencies identified in test, and the associated analysis and reports. The T&E WIPT defines the data requirements and T&E resources needed to adequately plan and execute the T&E program. The PM, collaborating and consulting with the T&E WIPT, should include T&E requirements in Requests for Proposals (RFPs) and acquisition contracts to ensure government access to the data needed to mitigate risk and inform key program decisions. In addition to contracts, the T&E WIPT should participate in acquisition program requirements refinement to ensure that they are measurable, testable, achievable and relevant to the operational mission. The PM should assist the T&E WIPT to consult with the requirements authority to clarify requirements that may not be testable.

The T&E WIPT includes representatives from all organizations responsible for providing or overseeing the T&E Strategy development and its execution. In particular, the T&E WIPT should include representatives of test data stakeholders such as systems engineering, DT&E, OT&E, LFT&E, the user, product support, the Intelligence Community, and applicable certification authorities. The T&E WIPT should enable collaboration among stakeholders to maximize efficiency by planning and executing an integrated T&E program that leverages all test events for the purposes of meeting developmental, live fire, and operational evaluation objectives. The PM should ensure that results from all test events are captured in a shared data repository (discussed below) and available for all parties to use for independent assessment.

- T&E WIPTs should be involved from the inception of the program to help define the T&E requirements captured in acquisition contacts and the associated data.
- T&E WIPTs should strive to maintain a tempo that supports the required decisions using various tools (e.g., digital engineering, sequential testing, automation).
- T&E WIPTs should develop a robust T&E program to support the milestone decisions with end-to-end mission threads employing actual users.
- OT&E and LFT&E should concentrate on appropriately scoped, dedicated tests while integrating useable data and information from all sources to meet stakeholder needs, support operational evaluations, and inform decisions.
- T&E WIPT may develop collaborative test data scoring boards to evaluate and authenticate any available test data for potential to meet any IOT&E and LFT&E requirements.

2.2 Test and Evaluation Planning for Middle Tier of Acquisition

The purpose of T&E planning is to define an executable strategy to adequately evaluate systems throughout the program's lifecycle for technical, functional, and operational capability to enable delivery of a system that meets the operational users' needs. As the planning process is critical and sets the conditions for success, all test teams should be involved early in the program during the planning process to establish and document how testing, modeling and simulation (M&S),

[14] Different naming convention for the T&E WIPT such as Integrated Test Team are common and acceptable. This document will refer to any of these as the T&E WIPT.

analysis, and evaluation of performance at its various maturity stages will be accomplished. The T&E WIPT should identify the measures to be used to evaluate the system as a part of the planning process, and then the data needed and conditions under which those data will be collected. A tabletop exercise can assist in confirming the feasibility of the proposed plans, tools, and methodology prior to inclusion in the T&E Strategy.

T&E planning should be digitized and automated as much as possible to support continuous development, integration, and delivery of system capabilities. Digital test management tools automate the process of test planning, scheduling, tracking, and reporting test events.

During the planning process, various stakeholders are developing documentation, summarized and defined in Table 2, to include the associated testing resources, tools, data, and infrastructure.

Table 2. Planning Documents

Artifact	Description	Developed by
Tailored Test and Evaluation Strategy[15]	Defines the processes by which technical, functional, and operational performance will be tested and evaluated to satisfy developmental test and evaluation criteria, and to measure technological maturity and prototype performance, as well as a description of how the program will achieve a residual operational capability.	Program Manager with support from T&E WIPT
Requirements	Specifies the requirements for the system to deliver the capability that meets needs specified by the Joint Chiefs of Staff and Combatant Commanders.	Sponsor with support from the Program Manager
Acquisition Strategy	An integrated plan that identifies the overall approach to acquiring, developing, delivering, and sustaining capabilities to meet users' needs.	Program Manager
Cost Estimate	Developed in accordance with DoDI 5000.73 (Cost Analysis Guidance and Procedures). The estimate should consider the technical content of the program described in the Capability Needs Statement (CNS), User Agreement (UA), Acquisition Strategy, and test strategy.	Program Manager

[15] Different naming conventions for the T&E Strategy are common (i.e. test strategy, Test and Evaluation Master Plan (TEMP), Simplified Acquisition Master Plan (SAMP)). Regardless of name, this document can be tailored and should be submitted for DOT&E for approval for programs on the T&E oversight list.

Artifact	Description	Developed by
Intellectual Property (IP) Strategy	Identifies and describes the management of delivery and associated license rights for all software and related materials necessary to meet operational, cybersecurity, and supportability requirements. The IP strategy should support and be consistent with all other government strategies for design, development, test and evaluation, operation, modernization, long-term supportability of the software, and protection of the software supply chain, and should be implemented via appropriate requirements in the contracts.	Program Manager
Request for Proposal	A document used in negotiated acquisitions to communicate government requirements, including those for T&E, to prospective contractors, and to solicit proposals.	Program Manager

2.2.1 T&E Content and Interests in Planning Documents

While the T&E Strategy is the main testing document for either the rapid prototyping or rapid fielding pathway, the success of T&E relies heavily on each of the other documents discussed below. The T&E community should work with the acquisition community on these documents to incorporate needed T&E information. This section highlights T&E content and involvement of test teams in the development of each of these documents.

2.2.2.1 Tailored Test & Evaluation Strategy

The purpose of documenting the T&E Strategy is to guide the activities of test organizations in planning and executing an effective and efficient test process in support of the outcome determination. The T&E Strategy serves as an agreement between the PM and all the T&E stakeholders for T&E roles and responsibilities, and resources, and should enable the evaluation of the unit equipped with the system executing the missions the system is intended to perform while considering all interfacing systems, threats, and operational environments. The T&E WIPT, guided by appropriate threat modules from the Defense Intelligence Threat Library, identifies threat adequacy for test.

The T&E WIPT should ensure the T&E Strategy is executable and aligns with the Acquisition Strategy, T&E policy (DODI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. Per the DoDI 5000.89, the T&E Strategy will include an Integrated Decision Support Key (IDSK), a table that outlines the acquisition, technical, and program decisions and the data (e.g., CT, DT, LFT, OT, M&S) necessary to support those decisions. The IDSK provides a framework for how test events can build on one another and support the data requirements for multiple stakeholders' evaluations simultaneously, producing efficiencies across the T&E lifecycle and facilitating the integration of DT, CT, and OT. The IDSK should evolve

and adapt as the system matures, and identify opportunities to incorporate operational realism (e.g., mission environments and operational users) as early as possible. Incorporating operational realism early in the test program improves the probability of identifying and correcting problems early, which is especially critical for MTA programs executed on short timelines. This approach facilitates a tailorable DT, OT, and LF approach that may affect the scope of individual test events. Stakeholders can pull data from prior events to support their evaluations. The T&E Strategy should describe how these data will be accumulated to build a shared body of evidence to support evaluations of the system (e.g.., data repository).

The T&E Strategy should define the conditions under which required data will be collected, and any tools required to manage the data and perform the testing. OT should consider informing the DT community of their OT data requirements to meet their evaluation objectives, and vice versa. As such, DT should consider the operational relevance of the developmental tests to identify operationally representative deficiencies sooner.

Embedding OT&E earlier in the program's lifecycle requires OT&E awareness and participation in the activity of the system development. This includes monitoring the tests that occur throughout the development and understanding the pedigree of the developmental testing to determine which results may be useable for operational evaluation. The test community must determine the applicability of prior data for OT&E, including the mapping of that data to the evaluation assessment areas, and identify gaps in data that will inform test planning for future iterations.

The DA approves the T&E Strategy, ensuring that it is executable and aligns with the Acquisition Strategy and the Acquisition Decision Memorandum (ADM). For programs on OSD T&E oversight, DOT&E is the final approval authority for the T&E Strategy.[16] The T&E Strategy will be submitted to the DOT&E for approval no later than 45 calendar days before the program start.

2.2.2.2 Requirements

The T&E WIPT should be involved with requirement development early to fully understand the desired capabilities and help inform how certain aspects of system design (e.g., cybersecurity) will be evaluated. The T&E WIPT should assist in the necessarily rapid definition of requirements that are clear, testable, and measurable. Test teams should:

- Understand what constitutes either a residual operational capability or mission effectiveness, suitability, survivability, and lethality, and how that should be evaluated consistent with the compressed schedules used for MTA programs
- Collaborate with stakeholders to help assure cyber and interoperability needs are rapidly identified and clearly defined, consistent with the MTA program schedules

2.2.2.3 Acquisition Strategy

The Acquisition Strategy should describe the MTA program and associated decisions sufficiently to convey what information/data testing needs to provide, and when to adequately support the

[16] DoDI 5000.89, November 19, 2020, pg. 5

transition decisions and evaluate the technical, functional, and operational performance as appropriate. The strategy should account for T&E when identifying resource needs. The Acquisition Strategy sets the schedule for delivering the capability. Test teams should collaborate rapidly and efficiently with stakeholders to help:

- Include the appropriate T&E-related provisions are included in RFPs and contracts
- Assure that adequate time is allotted in schedules to conduct the T&E needed to rapidly identify and fix key deficiencies.

2.2.2.4 Cost Estimate

The cost estimate should consider the technical content of the program described in the requirements document, Acquisition Strategy, and T&E Strategy. Test teams should collaborate to assure that the cost estimate includes all the resources necessary to plan and execute the T&E consistent with rapid prototyping or rapid fielding.

2.2.2.5 Intellectual Property (IP) Strategy

The IP strategy will identify and describe the management of delivery and associated license rights for all hardware, software, and related materials necessary to meet operational, cyber, and supportability requirements. It should include, to the maximum extent practicable for an MTA program, delivery of and access to the computer code, automated tools, and data needed to conduct T&E consistent with the schedule for rapid fielding or prototyping.

Test teams should provide input to the IP strategy on the rights of data generated (such as contractor-generated test results) during all phases of testing that would allow building a shared body of test evidence, available throughout the program's lifecycle. The PM should consult with the T&E community to determine any access needed to support independent testing and include these accesses in the IP strategy as needed.

2.2.2.6 Request for Proposal (RFP)

The RFP defines what the government expects from the contractor. If T&E expectations are not explicitly stated in the RFP and the acquisition contract, needed data will not be provided, increasing risk to the T&E program and potentially the entire program's cost and schedule. The T&E Strategy is a source document for the RFP and should be generated in time to support RFP development. A draft T&E Strategy should be included as an attachment to the RFP to inform contractors of the anticipated T&E activities and associated data. Test teams should work collaboratively and efficiently with the appropriate stakeholders to define the contract deliverables supporting the T&E Strategy that should be included in the RFP.

2.2.2 T&E Resources

The T&E Strategy should document the T&E resources required to support DT&E, OT&E, and LFT&E. Programs should identify one-of-a-kind T&E resources and long-lead items early in the acquisition process to allocate adequate funding for development and use. The lead test organizations should verify and validate the tools planned for OT&E use before the program enters execution. This verification and validation should consider data collection, interfacing systems and databases, networks, simulated environments, simulated users, and ranges. These resources include, but are not limited to:

- **Test articles (e.g., the system under test, test targets and expendables, threats, spares)**
  The environments used to conduct testing for OT&E should be as operationally realistic as possible, including realistic system use and threats. This requires the identification and inclusion of interfacing systems that form the system of systems.

- **Test facilities, infrastructure, instrumentation, and ranges, to include cyber ranges and test team, software integration laboratories**
  Programs should use government T&E capabilities unless an exception can be justified as cost-effective to the government. PMs will conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the T&E Strategy approval process before acquiring or using non-government test facilities or resources.

  The T&E Strategy should include any proposed use or application of embedded instrumentation. The intent of embedded instrumentation is to facilitate data collection and system diagnostics without modifying the system's operational configuration. The PM should work with the T&E WIPT and other stakeholders to plan for the of use embedded instrumentation to collect system performance and diagnostic data whenever feasible and should work to obtain accreditation and certification prior to use in OT&E. This may include adding requirements for these embedded instrumentation in program RFPs and other resourcing provisions.

  The PM should work with the T&E stakeholders for all test infrastructure and instrumentation that support the outcome determinations to be verified and validated by the intended user or appropriate accreditation agency.

- **Automated testing tools**
  Automated test execution tools may be a part of the process of executing test cases or procedures on the system under test. The T&E WIPT and PM should work with the contractor to fully understand the contractor's tools, specifically their verification and validation plans, and the credibility of those tools for the intended use. The automated tools should be structured to provide visibility into the continuous testing occurring within the development and fielding processes, as appropriate to the MTA approach, so that stakeholders can gain confidence as quickly as possible that the program will succeed. It is encouraged that government test teams be able to use these tools as appropriate so they can use their outputs to inform evaluations. Using the same tools as the contractor is advantageous for the government (e.g., easier to replicate events when necessary); provisions enabling this should be included in acquisition contracts. In some cases, government test teams must become experts in the tools used by both the contractor and government. Such expectations should be clarified with the appropriate contractual provisions.

- **M&S, and their verification and validation plans**
  The T&E Strategy should document initial versions of system M&S tools to be matured during development for use by government test organizations. These may include initial

digital system models, component level reliability and availability models, or other M&S tools. The PM, in collaboration with the T&E WIPT, should also consider whether the delivery of these tools, when applicable, should be included in the program RFPs.

The M&S strategy and schedule, including the using organization, intended use, and the commitment to provide a verification and validation plan for each tool or test infrastructure asset, should be documented in the T&E Strategy. The T&E Strategy should specify when particular T&E resources are required, and which organization is responsible for verification and validation, and for providing the associated resources.

- **Manpower and personnel**
  The T&E Strategy should include information about friendly and threat operational forces, data collectors, and subject matter experts that will be required to execute the T&E program.

- **Federal/State/local requirements, range requirements, and any special requirements**
  This may include requirements for explosive ordnance disposal, corrosion prevention and control, or frequency management and control.
- **Projected and actual level of funding to execute the required test program**
  Pursuant to Section 839(b) of Public Law 115-91, the PM should include a table in the T&E Strategy that lists the initial resource estimates for government DT&E, OT&E, and LFT&E. T&E funding in the resources section should be consistent with the cost estimate and budget submissions.
- **Data Repositories**
  During the MTA planning, the PM should establish a shared data repository to store test and evaluation data and provide access to all test teams so that they can review, use, and input these test data to meet their objectives. This should enable the use of sequential testing, big data analytics, and other adaptive methods in support of the IDSK and T&E efficiencies. Throughout system development, T&E should be building a shared body of test evidence to support efficient technical, functional, and operational performance evaluations and adaptive T&E. Relevant test data gathered through all testing should be included in this test data repository. To enable adequate use of sequential testing and similar T&E planning and analysis methods, the T&E WIPT should leverage existing or develop collaborative test data scoring boards to evaluate integrated test data for potential to meet operational or live fire requirements prior to the operational demonstration. It is possible to collect useful OT data across all planned and executed test events. The OTA should maintain the authoritative source of data authenticated to meet OT&E requirements.

3. T&E During MTA Pathway

3.1 Rapid Prototyping

Specific T&E activities within the Rapid Prototyping Pathway include:

- Generate the T&E Strategy
- Assist in including T&E requirements in the RFP
- Conduct developmental T&E
- Conduct an operational demonstration (ops demo)
- Conduct LFT&E (if applicable)
- Deliver a report
- Inform the outcome determination and transition decision

3.1.1 Generate the T&E Strategy

In coordination with the PM, the T&E WIPT should develop and document the T&E Strategy before starting the MTA program. For programs on the Rapid Prototyping pathway, the T&E Strategy should describe the data and testing necessary to measure technology maturity and performance and achieve a residual operational capability. The T&E Strategy should be complete enough to estimate and plan for the major resources required for adequate T&E consistent with the program's requirements and intended use. The T&E Strategy should document any risks to conducting adequate T&E and describe how those risks will be mitigated. To the extent possible, the T&E Strategy should:

- Present an IDSK that links data requirements for DT&E, OT&E, LFT&E
- Describe the evaluation focus areas and evaluation framework to meet DT&E, OT&E, and LFT&E, to include cyber T&E objectives
- Present an integrated program schedule that documents the test events
- Describe each test phase or event, to include how any test limitations will affect the evaluation
- Identify key T&E resources and projected level of funding for those resources (e.g., target sets, ranges, threat emulators, threat M&S, intelligence mission data)
- If applicable, specify the baseline against which the new system will be judged
- Identify key responsible T&E stakeholders, to include stakeholders responsible for verification and validation of proposed digital tools

3.1.2 Conduct Developmental T&E

The goal of DT&E is to manage and mitigate risk during development, verify system compliance with contractual and technical requirements, prepare for operational test (OT), inform decision makers throughout the program life cycle, and assess whether the integrated system provides military utility for the warfighter. Contractor DT&E should focus on test, fix, and retest of critical findings to mitigate risk to the program's cost, performance, and schedule consistent with the intent to rapidly prototype or field. Government testers should continue to leverage contractor-conducted DT&E to supplement government DT&E to assess:

- System capabilities and limitations per system specifications
- System safety and survivability, if applicable
- System ability to integrate within the operational environment
- The extent to which the contractor has mitigated any critical findings that have been discovered

- System ability to sustain mission capability and remain operationally resilient in a cyber-contested environment

Government developmental testing should also include prototype experimentation. Rather than simply demonstrating that a capability meets the need it was built to meet, experimentation should stress the technology to identify its full capabilities and limitations. In addition to evaluating the technical feasibility of a prototype, experimentation can also identify military utility and help in the development of preliminary CONOPS and tactics, techniques, and procedures for emerging technological capabilities.

The USD(R&E) will conduct DT&E Assessments for MTAs on the T&E Oversight List to support the Outcome Determination decision and any other key decision point(s) in the MTA effort, or as requested by the DA or PM. The assessment will address the adequacy of the program T&E planning, and the implications of T&E results to date.

3.1.3 Conduct Operational Test and Evaluation

The lead OTA will execute an ops demo at the culmination of the rapid prototyping phase to support the outcome determination. The purpose of an ops demo is to assess the technical maturity and interoperability of the system, as well as characterize a system's risk toward operational effectiveness, suitability, and survivability in a threat-realistic operational environment, as well as the system's capability and limitations.

The lead OTA will plan and conduct the ops demo with representative units, missions, and environments. Ops demos may consist of a series of incremental test events or a separate "capstone" demonstration event. Whenever possible, events should be conducted in an integrated fashion, supported by collaboration with the developer, Program Office, DT, and OT agencies and representative operational end users.

Ops demos should consider all aspects of system performance, including survivability and lethality, if deemed critical to mission effectiveness or force protection. During the ops demo, representative operational users should operate the system, with the minimum necessary level of contractor support. Mission demonstrations should consider operational missions, end-to end/system of systems mission kill chains and mission threads, and intended operating environments.

Operational T&E for an MTA Rapid Prototyping pathway program should ensure that systems function as intended, mitigating risks associated with known and exploitable vulnerabilities to provide a level of assurance commensurate with technology, program, system, and mission objectives.

For programs on the T&E Oversight List, the OTA must submit the ops demo plan to the DOT&E for approval before testing begins. For programs conducting multiple ops demos, DOT&E will tailor this approval process to minimize disruptions during early testing. Programs not on T&E oversight should follow guidance provided by their Service. Plans for ops demos should adequately describe system configuration, capabilities to be demonstrated, the operational units, users, mission, and environment, and the primary T&E data that will demonstrate the required capabilities.

The OTA supports the outcome determination and transition decision by reporting the findings of T&E activities, to include the system's operational capabilities and limitations. For programs on DOT&E oversight, the Director, Operational Test and Evaluation provides the Defense Acquisition Executive (DAE), the Secretary of Defense, the Service, the DA, and Congress with an independent report documenting the results of T&E activities, including capabilities and limitations of the system and its ability to provide a residual operational capability. For programs only on LFT&E oversight, the Director will submit a report at the conclusion of survivability or lethality testing.

3.1.4 Conduct Live Fire Test and Evaluation

Programs that intend to field rapid capabilities are not exempt from the requirements of 10 U.S.C. §§ 4172 to conduct "realistic survivability testing" or "realistic lethality testing" before proceeding to outcome determination. Early live fire testing of new technologies is critical to ensuring a timely evaluation of the survivability or lethality of a system as it progresses through design, prototyping, and fielding. In particular, LFT&E:

- Provides information to decision makers on potential user susceptibility to an attack, design vulnerabilities if engaged, and the effect of those vulnerabilities on user casualties, as well as residual mission capability post-engagement and recoverability from an attack
- For weapon systems or weaponized platforms, it provides information on lethality while taking into equal consideration the survivability of the weapon system as it is employed against its target
- Ensures testing of the system under realistic combat conditions

LFT&E occurs over the course of a rapid prototyping phase, beginning with component-level and sub-system and system-level testing during the initial design stage, warhead characterization of new threats, and M&S-based assessment. T&E continues as the system matures from assemblies to sub-systems, and finally to full-up, system-level (FUSL). During FUSL testing, the weapon system is powered and fully equipped for combat with all sub-systems operational. For programs that intend to transition into operational use, rapid fielding, or an existing program, a decision about whether to request a waiver from FUSL testing should be made before rapid prototyping to allow for submission of the waiver package to Congress. The statute states that any waiver must be approved prior to the start of prototype development, or as soon as is practicable after program initiation, depending on the specifics of the acquisition schedule for a given system. The waiver package sent to Congress consists of two parts: 1) certification that the waiver is needed (on the basis of both cost and practicality), and 2) an alternative LFT&E plan for evaluating survivability or lethality. These two parts require coordination between the acquisition executive and DOT&E. After test completion, DOT&E will produce an LFT&E Report, combined with the Operational Assessment Report. The OTA provides an independent report. For programs on DOT&E oversight, the OTA provides these reports to DOT&E. (DoDI, November 19, 2020 Section 6.4.c).

3.1.5 Informing the Outcome Determination and Transition Decision

For each MTA program, DoD Components will make a transition decision or outcome determination at the conclusion of the phase. The T&E WIPT and independent T&E organizations provide the information gained from DT&E, OT&E, and LFT&E to support the decision, which could include the following courses of action available:

- **Prototype is Discarded and Program is terminated.** The prototype built is the simplest and least expensive prototype possible that answers the required question and has no further utility.
- **Residual operational capability sustained in the field.** Prototypes will transition to operational use to address an existing critical warfighter capability gap.
- **Transition to Rapid Fielding Pathway.** The MTA pathway can authorize a rapid fielding pathway for prototypes that meet a high-priority warfighter need or reduces the lifecycle cost of a weapon system. Production using this pathway is expected to begin within six months and completed within five years.
- **Transition to new or existing Program in a different acquisition pathway.** Some prototyping projects are designed to develop new technology that will integrate into an MCA or an existing fielded Program of Record as a component or subcomponent of the larger system.

3.1.6 Deliver a Rapid Prototyping Report

At decision points identified in the T&E Strategy, a report will be provided to the DA on the current state of capabilities, system integration, operational effectiveness, suitability, survivability, and lethality (if required), and sustainment. The OTA is responsible for producing an independent evaluation report(s) identifying the system's operational capabilities and limitations. The DA will use the report(s) in determining if a rapid prototyping program transitions to a follow-on program. For programs on DOT&E oversight, the Director, Operational Test and Evaluation will provide independent operational assessment and LFT&E reports to the Office of the Secretary of Defense, Joint Staff, Military Services, and congressional defense committees.

3.2 Rapid Fielding

Key T&E activities in the Rapid Fielding pathway include:

- Generate the T&E Strategy
- Assist in including T&E needs in the RFP
- Conduct developmental T&E
- Conduct operational T&E
- Conduct LFT&E (if applicable)
- Deliver a Rapid Fielding Report
- Inform the outcome determination and the transition decision

3.2.1 Generate the T&E Strategy

In coordination with the PM, the T&E WIPT should develop and document the T&E Strategy before starting the MTA program. For program transitions from the rapid prototyping pathway, a new or updated T&E Strategy should be generated. For programs on the Rapid Fielding pathway, the T&E Strategy documents the data and resources necessary to demonstrate performance of the proposed products or technology for current operational purposes and how the capability contributes to mission accomplishment. The T&E Strategy should be complete enough to estimate and plan for the major resources required for adequate T&E in accordance with the requirements outlined in the requirements document. The T&E Strategy should document any risks conducting adequate T&E and describe how those risks will be mitigated. To the extent possible, the T&E Strategy should:

- Present an IDSK that links data requirements for DT&E, OT&E, LFT&E, to include cyber T&E to key program decisions
- Describe the evaluation focus areas and evaluation framework to meet DT&E, OT&E, and LFT&E, to include cyber T&E objectives
- Present an integrated program schedule that documents the test events
- Describe each test phase or event
- Identify key T&E resources and funding for those resources (e.g., target sets, ranges, threat emulators, threat M&S, intelligence mission data)
- If applicable, specify the baseline against which the new system will be judged and the resources allocated for the baseline testing
- Identify key responsible T&E stakeholders, to include stakeholders responsible for verification and validation of proposed digital tools

3.2.2 Conduct Developmental T&E

Rapid fielding efforts are intended for systems or upgrades with little to no development required. However, the government will need information on the extent to which the integrated system provides the required capabilities and can be sustained in operations. The program executes government DT&E to assess:

- System capabilities and limitations per system specifications
- System safety and survivability, if applicable
- System ability to integrate within the operational environment
- The extent to which the contractor has mitigated any critical findings
- System ability to sustain mission capability and remain operationally resilient in a cyber-contested environment
- Whether production processes have been refined and are acceptable

Government testers should leverage contractor-conducted DT&E to supplement government DT&E. Production Qualification Testing (PQT), First Article Testing (FAT), and Acceptance Testing (AT) are normally conducted either by Program Management Office personnel or by the contractor using government-approved test plans and under the oversight of government personnel resident at the contractor facility.

FAT evaluates how production processes and environmental stress affect system performance, and should be conducted expeditiously because the production line may continue to flow while results are analyzed.

AT ensures that each system from the production line functions properly, and is critical because it is the point where the government accepts ownership and responsibility of the system and may also be the date on which warranty coverage begins.

PQT could also be warranted where new or modified production processes or materials are used. PQT ensures the effectiveness of the manufacturing process, equipment, and procedures, and provides data for the independent evaluation required for materiel release so that the evaluator can address the adequacy of the materiel with respect to the stated requirements. These tests are conducted on a number of samples taken at random from the first production lot and is repeated if the process or design is changed significantly and when a second or alternative source is brought on-line.

3.2.3 Conduct Operational Test and Evaluation (OT&E)

Operational T&E for a rapid fielding pathway program should ensure that systems function as intended, mitigating risks associated with known and exploitable vulnerabilities. OT&E should provide a level of assurance commensurate with technology, program, system, and mission objectives for the rapid fielding pathway program. There are several options for operational testing of rapid fielding programs, which may include:

- **Initial Operational Test & Evaluation (IOT&E).** An IOT&E is appropriate for MTAs requiring a full-rate production decision.
- **Operational Assessment (OA).** An OA is appropriate for reducing program risk, demonstrating system performance, and identifying key potential user, interface, and operational usage issues to reduce risk of finding major issues during IOT&E.
- **Ops Demo.** An Ops Demo is appropriate for MTAs integrating into an existing program of record or for MTAs transitioning to a new or existing program in a different acquisition pathway.

Operational T&E activities may use production or production-representative test articles (depending on the type of OT&E and whether a full-rate production decision is planned) to assess the rapid fielding system's operational effectiveness, suitability, survivability, and lethality, if applicable. OT&E activities require more than an evaluation based exclusively on computer modeling, simulation, or an analysis of system requirements, engineering proposals, design specifications, or any other information contained in program documents. OT&E should feature end-to-end testing of system capabilities, including all interrelated systems needed to employ and support those capabilities. OT&E should include representative users or units employing the system under conditions simulating combat stress, and if applicable, peacetime operations. Individuals employed by the contractor for the system being developed should only participate in OT&E to the extent they are planned to be involved in the operation, maintenance, and other support of the system when deployed in combat. The OTA supports the outcome determination and transition decision by reporting the findings of T&E activities, to include the system's operational performance.

The lead OTA conducts operational T&E activities in accordance with a test plan approved by DOT&E for programs on DOT&E oversight.

3.2.4 Conduct Live Fire Test & Evaluation

Rapid fielding pathway programs are not exempt from 10 U.S.C. §§ 4172 and should conduct realistic survivability and lethality testing before proceeding to outcome determination. Realistic survivability testing means testing for the susceptibility, vulnerability, force protection, and recoverability of the system and its crew in a contested operational environment using adversary-representative threats fired against the production-representative system equipped with any available countermeasures. Realistic lethality testing means testing for lethality by engaging the production-representative weapon against adversary-representative targets configured for combat equipped with any associated countermeasures.

Early live fire testing of new technologies is critical to ensure a timely evaluation of the survivability or lethality of a system as it progresses through its lifecycle. In particular, LFT&E:

- Provides information to decision makers on potential user susceptibility to an attack, design vulnerabilities if engaged and the effect of those vulnerabilities on user casualties, as well as residual mission capability post engagement and recoverability from an attack
- For weapon systems or weaponized platforms, it provides information on lethality while taking into equal consideration the survivability of the weapon system as it travels to its target
- Ensures testing of the system under realistic combat conditions

LFT&E should occur over the course of a rapid fielding phase, beginning with component-level and sub-system and system-level testing during the initial design stage with warhead characterization of new threats and M&S based assessment. T&E continues as the system matures from assemblies to sub-systems, and finally to full-up, system-level (FUSL). During FUSL testing, the weapon system is powered and fully equipped for combat with all sub-systems operational.

Although there is no waiver from LFT&E, the law contains provisions for a waiver from the requirements for FUSL testing. The Secretary of Defense may waive the application of the required FUSL testing if the Secretary determines that such testing would be unreasonably expensive and impractical. The waiver package sent to Congress consists of two parts: 1) certification that the waiver is needed (on the basis of both cost and practicality), and 2) an alternative LFT&E plan for evaluating survivability or lethality. These two parts require coordination between the acquisition executive and DOT&E.

DOT&E approves LFT&E plans for select live fire test events, as identified in the T&E Strategy. The document approval matrix in the T&E Strategy specifies which planning documents will be submitted for DOT&E approval and which will be submitted for information and review only. The Service OTA or assigned test activity conducts LFT&E events, executing the planned events in accordance with the LFT&E Strategy and approved LFT&E Plan.

After test completion, DOT&E will produce an LFT&E Report, combined with the Operational Assessment Report. The OTA provides an independent report. For programs on DOT&E oversight, the OTA provides these reports to DOT&E. (DoDI 5000.89, November 19, 2020 Section 6.4.c).

3.2.5 Informing the Outcome Determination and Transition Decision

For each MTA program, the DA will make a transition decision or outcome determination at the conclusion of the effort. The information gained from DT&E, OT&E, and LFT&E supports those decisions. There are three distinct follow-on courses of action for programs:

- **Transition to Operations and Sustainment.** Programs will transition to operations and sustainment use to address an existing critical warfighter capability gap.
- **Integration into an Existing MCA.** Some programs are designed to integrate into an existing MCA as a component or subcomponent of the larger system.
- **Transition into a New or Existing Program of Record in a different acquisition pathway.** Some programs may initiate a new program using the MCA pathway and entering at Milestone C to produce a higher quantity of the production articles or integrate into an existing MCA as a component or subcomponent of the larger system.

MTA programs may not be planned to exceed five years to completion and, in execution, will not exceed five years after MTA program start without a DAE waiver.

3.2.6 Deliver a Rapid Fielding Report

At decision points identified in the T&E Strategy, a report will be provided to the DA on the current state of capabilities, system integration, operational effectiveness, suitability, survivability, and lethality (if required), and sustainment. The OTA is responsible for producing an independent evaluation report(s) identifying the system's operational capabilities and limitations. The DA will use the report(s) in determining if a rapid fielding program transitions to a follow-on program, or if it begins initial production. For DOT&E oversight programs, the Service OTA provides the report to DOT&E. For programs on DOT&E oversight, the Director, Operational Test and Evaluation will provide independent OT&E and/or LFT&E reports to the DA, Office of the Secretary of Defense, Joint Staff, Military Services, and congressional defense committees.

TEST AND EVALUATION CHAPTER 4: MAJOR CAPABILITY ACQUISITION

Table of Contents

1. Major Capability Acquisition (MCA) Pathway Overview

1.1 Introduction

In accordance with DoDI 5000.02, the DoDI 5000.85 establishes policy and prescribes procedures that guide the acquisition of Major Capability Acquisition Pathway programs, including Major Defense Acquisition Programs (MDAPs); other programs categorized as Acquisition Category (ACAT) I; major systems, usually categorized as ACAT II; automated information systems (AIS) (not managed by other acquisition pathways); and other capabilities developed via the MCA Pathway. The guidance provided here supports policy established in the DoDI 5000.85, DoDI 5000.88 and DoDI 5000.89. In the event of conflict, the reader should defer to policy documentation. The Milestone Decision Authority (MDA) should structure program strategies, phase content, the timing and scope of decision reviews, and decision levels based on the specifics of the product being acquired, including complexity, risk, security, and urgency to satisfy validated capability requirements.

The Program Manager (PM) should involve the T&E organizations with the acquisition program from its inception (at the Materiel Development Decision) and throughout its lifecycle to support the program decisions and delivery timeline. Contractor testing (CT), government developmental test and evaluation (DT&E), live fire test and evaluation (LFT&E), and operational test and evaluation (OT&E) should be integrated, streamlined, and automated to the maximum extent practicable to enable efficient use of data and resources across the test program and evaluation of system operational effectiveness, suitability, survivability, and lethality to inform the decision authorities. Maximum sharing, reciprocity, availability, and reuse of test results and artifacts among testing and certification organizations improve chances for a successful and efficient T&E program. Collaboration between all organizations should be considered to develop digital system models, simulations, and test environments for common use across the spectrum of system tests that may produce necessary data or information.

This chapter describes T&E community involvement throughout the MCA Pathway lifecycle.

1.2 Major Capability Acquisition Pathway Description

Figure 1 illustrates the five major phases within the MCA Pathway: 1) Materiel Solution Analysis, 2) Technology Maturation and Risk Reduction, 3) Engineering and Manufacturing Development, 4) Production and Deployment, and 5) Operations and Support. Each phase is discussed briefly below. Additional details about T&E community involvement during each phase are discussed in Section 2.

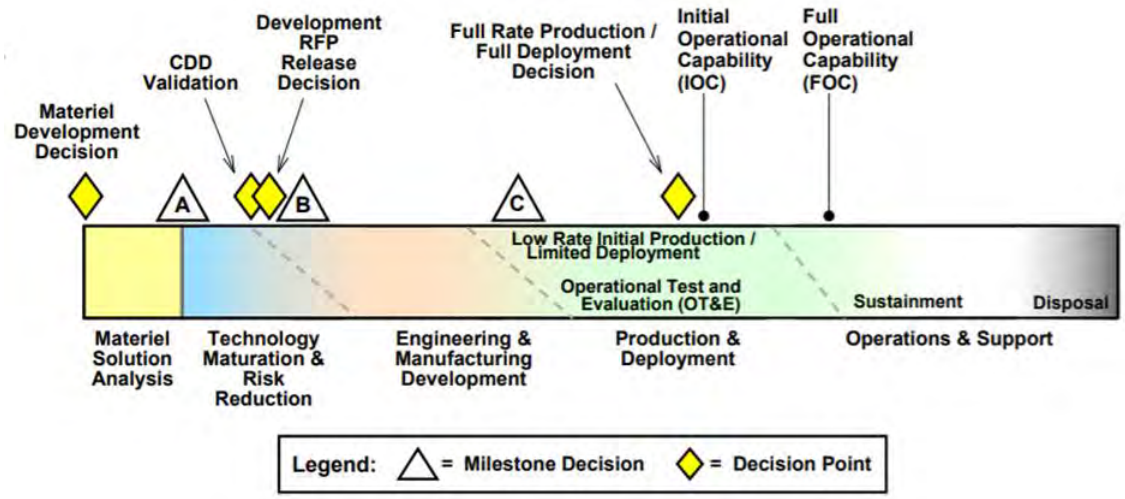


Figure 1. Major Capability Acquisition Pathway Phases[17]

1.2.1 Materiel Solution Analysis

The purpose of the Materiel Solution Analysis phase is to choose the concept for the system the DoD will acquire, begin translating validated capability gaps into system-specific requirements, and support a decision on the system's Acquisition Strategy. During this phase, the PM charters a T&E Working Integrated Product Team (WIPT), or equivalent entity, responsible for defining the T&E activities and requirements needed to support the Request for Proposal (RFP) and Milestone A decision.

The Milestone A decision approves program entry into the technology maturation and risk reduction (TMRR) phase, the program Acquisition Strategy, and release of the final RFPs for TMRR activities. An initial capabilities document (ICD) and test strategy should inform the Acquisition Strategy and the RFP for TMRR. Government test teams should be involved early in the program during this phase to establish and document how testing will be accomplished to adequately demonstrate the required technology maturity and assess the engineering, integration, and lifecycle cost risk.

1.2.2 Technology Maturation and Risk Reduction (TMRR)

The purpose of the TMRR phase is to mature technology and reduce technology, engineering, integration, and lifecycle cost risk, to the point that a decision to contract for Engineering and Manufacturing Development (EMD) can be made with confidence, leading to successful program execution for development, production, and sustainment. This phase includes a preliminary design review (PDR) and multiple competitive sources conducting technology risk reduction activity to demonstrate new technologies in a relevant environment. USD(R&E) or the DoD component will conduct an Independent Technical Risk Assessment (ITRA) that provides a view of program technical risk and their potential impacts to cost, schedule, and performance. The T&E community should

[17] DoDI 5000.85, August 6, 2020, p. 10.

collaborate closely during this phase to ensure the testability of the requirements outlined in the ICD, and include government T&E requirements in the development RFP that supports Milestone B to ensure access to contractor data and information that may improve the program's likelihood of success.

The Milestone B decision authorizes a program to enter into the EMD phase and commits the required investment resources to support the award of contracts. Government test teams should be involved early in this phase to establish and document how testing during the EMD phase will be accomplished in the Milestone B Test and Evaluation Master Plan (TEMP).

1.2.3 Engineering and Manufacturing Development

The purpose of the EMD phase is to develop, build, and test the system to determine the extent to which it meets operational, acquisition, and contractual requirements, and to support the program's production and deployment decisions. This phase includes a critical design review (CDR) and T&E to assess readiness to begin pre-production prototype hardware fabrication or software coding with acceptable risk. Government T&E should demonstrate the stability of the design, product compliance with contractual requirements, observed capabilities and limitations, any risks in meeting operational effectiveness, suitability, survivability, and lethality and the ability to achieve key performance parameters and key system attributes. Government T&E should be planned and executed in coordination with developmental, live fire, and operational test communities to efficiently and effectively uncover risks across the system's performance envelope and to assist the PM in managing those risks in support of the Milestone C Low-Rate Initial Production (LRIP) decision.

The Milestone C decision authorizes a program to enter the Production and Deployment phase, enter LRIP, and award production contracts.[18] In addition to the results of government T&E, the Milestone C decision review will also consider any significant manufacturing risk, the status of critical intelligence parameters and intelligence mission data requirements relative to fielding timelines, and full funding.

The T&E WIPT should consider the data collected during EMD to inform the updates to the Milestone C TEMP, another prerequisite for the Milestone C decision. The Milestone C TEMP should identify long lead items that need to be procured during this phase, which should be documented in the authorized Acquisition Decision Memorandum (ADM), along with any limits in content and/or dollar value. Examples of long lead items include number of targets, weapons, specialized range capabilities, etc. for LRIP or full-rate production T&E. The ADM should also document the LRIP quantities needed for T&E. While LRIP test assets need to be coordinated with DOT&E for programs on T&E oversight, for systems not on the T&E Oversight List, the OTA, following consultation with the PM, determines the number of test articles required for Initial Operational Test and Evaluation (IOT&E) (10 U.S.C. § 4231). The first Selected Acquisition Report submitted to Congress includes the LRIP quantity, with a rationale if it exceeds 10

[18] High cost articles such as ships will not produce prototypes during EMD for use solely as test articles. In such cases, the first article produced will be tested and evaluated, and then fielded as an operational asset.

percent of the total production quantity documented in the Acquisition Strategy (e.g., if the LRIP quantity is driven by the number of systems required to support IOT&E).

1.2.4 Production and Deployment

The purpose of the Production and Deployment phase is to deliver a system to military units that meets the intended operational capability and satisfies mission needs. The Production and Deployment includes LRIP, personnel training, completion of T&E intended to meet developmental assessment objectives, IOT&E, and the full-rate production (FRP) or full-deployment (FD) decision. IOT&E is a statutory test event requiring:

- Production-representative systems
- Operationally realistic units and users, missions, threats, environments, and maintenance activities in accordance with the system's fielding concept
- Adequate resources to ensure appropriately sized and operationally realistic testing
- A strategy for mitigating known test limitations

Programs should complete all planned testing and fix any identified critical system deficiencies prior to proceeding to IOT&E.

The MDA will conduct an FRP decision review to assess the results of IOT&E and initial manufacturing. Proceeding to FRP requires demonstrated control of the manufacturing process, acceptable operational performance, to include reliability, and the establishment of adequate sustainment and support systems. The FRP decision should also be informed by consideration of changes to the validated threat environments that might affect operational effectiveness, if they were not considered in IOT&E.

1.2.5 Operations and Support

The purpose of the Operations and Support phase is to execute the product support strategy, satisfy materiel readiness and operational performance requirements, including personnel training, and sustain the system over its lifecycle, including disposal, in the most cost-effective manner.

This phase includes two major efforts: sustainment and disposal. Effective sustainment results from designing and developing a supportable, reliable, and maintainable system. The PM works with system users to document performance and sustainment requirements in agreements specifying objective outcomes, measures, resource commitments, and stakeholder responsibilities. The Services, with system users, conduct continuing reviews of sustainment strategies to compare performance expectations against actual performance measures.

During this phase, the PM may initiate system modifications, as necessary, to improve performance and reduce ownership costs, and should formally inform test organizations of system modifications in time to prepare an adequate TEMP update to assess the effect of those modifications on operational performance. The PM should also consider the use of digital technology to enable continuous evaluation of more dynamic system changes (e.g., software) and threats (e.g., cyber) as both evolve over the life-cycle of the system.

At the end of its useful life, a system will be demilitarized and disposed in accordance with all legal and regulatory requirements and policy related to safety.

1.3 Major Capability Acquisition Pathway T&E Overview

Figure 2 summarizes the T&E events and associated products as the program progresses through the major phases and milestones of the MCA Pathway.

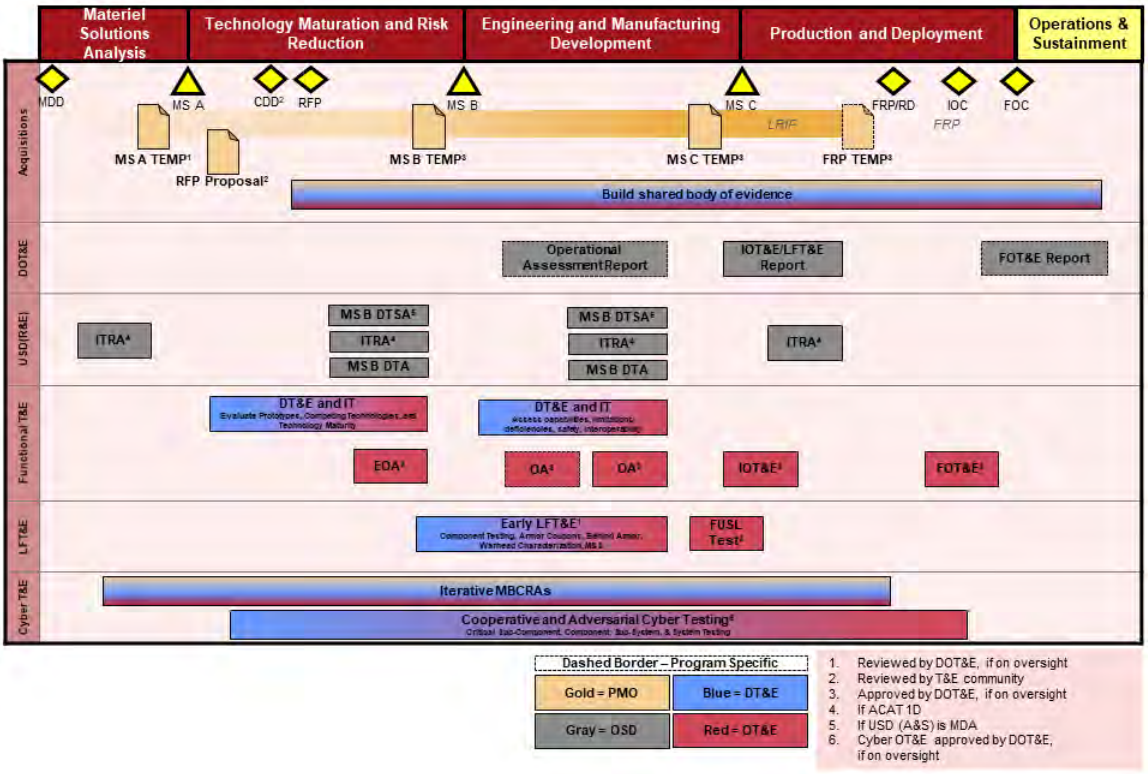


Figure 2. T&E Aligned with MCA Pathway

1.4 Test and Evaluation Working-level Integrated Product Team (WIPT)

The T&E WIPT coordinates top-level planning for all products and events listed in Figure 2 and the integrated schedule, which should account for the time needed to fix any deficiencies identified in test, and the associated analysis and reports. The T&E WIPT defines the data requirements and T&E resources needed to adequately plan and execute the T&E program. The PM, in collaboration and consultation with the T&E WIPT, should include the T&E requirements in RFPs and acquisition contracts to ensure government access to the data needed to inform key program decisions. In addition to contracts, the T&E WIPT should participate in acquisition program requirements refinement (e.g., ICD/CDD) to ensure the requirements' measurability, testability, achievability, and relevance to the operational mission. The PM should help the T&E WIPT coordinate with the requirements authority to clarify any requirements found untestable.

The T&E WIPT includes representatives from all organizations responsible for providing or overseeing development of the Test and Evaluation Master Plan (TEMP) and its execution. In particular, the T&E WIPT should include representatives of test data stakeholders such as systems engineering, DT&E, OT&E, LFT&E, the user, product support, the Intelligence Community, and applicable certification authorities. The T&E WIPT should enable collaboration among stakeholders to maximize efficiency by planning and executing an integrated T&E program that leverages all test events for the purposes of meeting developmental, live fire, and operational evaluation objectives. The PM should ensure that results from all test events are captured in a shared data repository (discussed below) and available for all parties to use for independent assessment.

- Government test teams should be involved from the inception of the program to ensure the T&E requirements are captured in acquisition contacts and the associated data.
- Government test teams should strive to maintain a tempo that supports the required decisions using various tools (e.g., digital engineering, sequential testing, automation).
- Government test teams should develop a robust T&E program to support the milestone decisions with end-to-end mission threads employing actual users.
- OT&E and LFT&E should concentrate on appropriately scoped, dedicated tests while integrating useable data and information from all sources to meet stakeholder needs, support operational evaluations, and inform decisions.
- T&E WIPT may develop collaborative test data scoring boards to evaluate and authenticate any available test data for potential to meet any IOT&E and LFT&E requirements.

Embedding OT&E earlier in the program's lifecycle requires OT&E awareness and participation in system engineering and system development. This includes monitoring the tests that occur throughout the development, and understanding and trusting the pedigree of the developmental testing to determine which results may be usable for operational evaluation. The test community should determine the applicability of prior data for OT&E, including the mapping of that data to the evaluation assessment areas, and identify gaps in data that will inform test planning for future iterations.

1.5 Test and Evaluation Planning for Major Capability Acquisition Pathway

The purpose of T&E planning is to better understand users' needs and define an executable approach to credibly demonstrate the technical, functional, and operational capabilities that need to be delivered to meet the users' needs. As the planning process is critical and sets the conditions for success, all test teams should be involved early in the program during the planning process to establish and document how testing, modeling and simulation (M&S), analysis, and evaluation of the system performance at its various maturity stages will be accomplished. The T&E WIPT should identify the measures to be used to evaluate the system as a part of the planning process, and then the data needed and conditions under which those data will be collected. A tabletop exercise can assist in confirming the feasibility of the proposed plans, tools, and methodology prior to inclusion in the TEMP.

T&E planning should be digitized and automated as much as possible to support continuous development, integration, and delivery of system capabilities. Digital test management tools automate the process of test planning, scheduling, tracking, and reporting test events.

During the planning process, various stakeholders are developing documentation, summarized and defined in Table 1, to include the associated testing resources, tools, data and infrastructure. The T&E community should work with the acquisition community on these documents to incorporate needed T&E information. This section highlights T&E content and involvement of test teams in the development of each of these documents.

Table 1. Planning Documents

Artifact	Description	Developed by
Test and Evaluation Master Plan (TEMP)	Defines the processes by which technical, functional, and operational performance will be tested and evaluated to satisfy developmental test and evaluation criteria, and to demonstrate operational effectiveness, suitability, survivability, and lethality.	Program Manager with support from T&E WIPT
Capability Development Document (CDD)	Specifies the operational requirements for the system to deliver the capability that meets operational performance criteria specified in the Initial Capabilities Document, which documents the need for a materiel approach to close a specific capability gap.	Sponsor with support from the Program Manager and T&E IPT
Acquisition Strategy	An integrated plan that identifies the overall approach to acquiring, developing, delivering, and sustaining capabilities to meet the users' needs.	Program Manager
Systems Engineering Plan (SEP)	Documents key technical risks, processes, resources, metrics (Technical Performance Measurement and other metrics), SE products, quality control, and completed or scheduled SE activities. The SEP is a living document, updated as needed to reflect the program's evolving SE approach and/or plans and current status.	Program Manager
Validated Online Life Cycle Threat (VOLT)	Serves as the authoritative, system-specific threat assessment tailored for and normally focused on one specific program. The VOLT involves the application of threat modules and is written to articulate the relevance of each module to a specific acquisition program or planned capability.	Intelligence Community

Artifact	Description	Developed by
Intellectual Property (IP) Strategy	Identifies and describes the management of delivery and associated license rights for all software and related materials necessary to meet operational, cybersecurity, and supportability requirements. The IP strategy should support and be consistent with all other government strategies for design, development, T&E, operation, modernization, and long-term supportability of the software, as well as protection of the software supply chain, and should be implemented via appropriate requirements in the contracts.	Program Manager
Cost Estimate	Developed in accordance with DoDI 5000.73 (Cost Analysis Guidance and Procedures). The estimate should consider the technical content of the program described in the Capability Needs Statement (CNS), User Agreement (UA), acquisition strategy, and test strategy.	Program Manager
Request for Proposal	A document used in negotiated acquisitions to communicate government requirements, including those for T&E, to prospective contractors and to solicit proposals.	Program Manager

1.5.1 Test and Evaluation Master Plan (TEMP)

The TEMP serves as an agreement between the PM and all T&E stakeholders describing the T&E program, including T&E roles and responsibilities, and resources. The TEMP captures the data requirements and processes by which the system will be tested and evaluated to verify technical requirements and to evaluate operational effectiveness, suitability, survivability, and lethality. The TEMP should enable the evaluation of the unit equipped with the system executing the missions the system is intended to perform while considering all interfacing systems, threats, and operational environments.

The T&E WIPT should ensure the TEMP is executable and aligns with the Acquisition Strategy, T&E policy (DoDI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. Per the DoDI 5000.89, the TEMP will include an Integrated Decision Support Key (IDSK), a table outlining the acquisition, technical, and program decisions as well as the data (e.g., CT, DT, LFT, OT, M&S) necessary to support those decisions. The IDSK provides a framework for how test events can build on one another and support the data requirements for multiple stakeholders' evaluations simultaneously, producing efficiencies across the T&E lifecycle and facilitating the integration of DT, CT, and OT. The IDSK should evolve and adapt through the system lifecycle and identify opportunities to incorporate operational realism (e.g., mission environments and

operational users) as early as possible. Incorporating operation realism early in the test program through integrated testing improves the probability of identifying and correcting problems early, rather than later in development, when redesigns are more expensive and correcting problems may prove infeasible. This approach does not support the replacement of dedicated DT&E, OT&E, or LFT&E, but may affect the scope of individual test events if stakeholders can pull data from prior events to support their evaluations. The TEMP should describe how these data will be collected to build a shared body of evidence to support evaluations of the system during the various acquisition phases.

The TEMP should define the conditions under which required data will be collected, and any tools required to manage the data and perform the testing. OT should consider informing the DT community of their OT data requirements to meet their evaluation objectives, and vice versa. As such, DT should consider the operational relevance of developmental tests to identify operationally representative deficiencies sooner in the acquisition cycle.

For programs on T&E oversight, DOT&E is the final approver for the TEMP.[19] At specified milestones, the TEMP is submitted to the Director for approval no later than 45 calendar days before the supported decision point. USD(R&E) is the approval authority for the DT&E plan in the TEMP for all ACAT ID programs. USD(R&E) reviews and advises the MDA on the DT&E plan in the TEMP for ACAT IB and IC programs. The TEMP should be updated as new data are collected and as the program reaches new acquisition milestones and decision points.

a. T&E Resources

The TEMP should document the T&E resources required to support DT&E, OT&E, and LFT&E. Programs should identify one-of-a-kind T&E resources and long-lead items early in the acquisition process to allocate adequate funding for development and use. The lead test organizations should verify and validate any applicable infrastructure, instrumentation, tools, and M&S planned for OT&E use before the program enters execution. This verification and validation should consider data collection, interfacing systems and databases, networks, simulated environments, simulated users, and ranges.

These resources may include, but are not limited to:

1) **Test articles (e.g., the system under test, test targets and expendables, threats)**

The environments used to conduct testing for OT&E should be as operationally realistic as possible, including realistic system use and threats. This requires identification and inclusion of the interfacing systems that form the system of systems with the program of record.

[19] DoDI 5000.89, November 19, 2020, pg. 5

2) **Test facilities, infrastructure, instrumentation, and ranges, to include cyber ranges and test team, software integration laboratories**

Programs should use government T&E capabilities unless an exception can be justified as cost-effective to the government. PMs will conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the TEMP approval process before acquiring or using non-government test facilities or resources.

The TEMP should include any proposed use or application of embedded instrumentation. The intent of embedded instrumentation is to facilitate data collection and system diagnostics without modifying the system's operational configuration. The PM should work with the T&E WIPT and other stakeholders to plan for the use of embedded instrumentation to collect system performance and diagnostic data whenever feasible, and to obtain accreditation and certification prior to use in OT&E. This may include adding requirements for these embedded instrumentation in program RFPs and other resourcing provisions.

The PM should work with the T&E stakeholders to enable all test infrastructure and instrumentation that supports acquisition decisions to be verified and validated by the intended user or appropriate accreditation agency.

3) **Automated testing tools**

Automated test execution tools may be a part of the process of executing test cases or procedures on the system under test. The T&E WIPT and PM should work with the contractor to fully understand the contractor's tools. The automated tools may provide visibility into the continuous testing occurring within the development process so that stakeholders can gain confidence in the quality of the development process. It is encouraged that government test teams be familiar with and capable of using these tools to inform whether credible use of the tools' outputs may inform evaluations. Using the same tools as the contractor is advantageous for the government (e.g., easier to replicate events when necessary) and should be included in the acquisition contract. In some cases, government test teams may become experts in the tools used by both the contractor and government. Such expectations should be clarified within the appropriate contractual provisions.

4) **M&S, and their verification and validation plans**

The TEMP should document initial and subsequent versions of system M&S tools to be matured during development for use by government test organizations during EMD and beyond. These may include initial digital system models, component-level reliability and availability models, or other M&S tools. The PM, in collaboration with the T&E WIPT, should also consider whether the delivery of these tools, when applicable, should be included in the program RFPs.

The M&S strategy and schedule, including the using organization, intended use, and the commitment to provide a verification and validation plan for each tool or test infrastructure asset, should be documented in the TEMP. The TEMP should specify when

particular T&E resources are required, and which organization is responsible for verification and validation, and for providing the associated resources.

5) **Manpower and personnel**

The TEMP should include information about friendly and threat operational forces, data collectors, and subject matter experts that will be required to execute the T&E program.

6) **Federal/State/local requirements, range requirements, and any special requirements**

This may include requirements for explosive ordnance disposal, corrosion prevention and control, or frequency management and control.

7) **Data repositories**

The TEMP should document a plan for a shared data repository. At program initiation, the PM should establish a shared data repository to store test and evaluation data and provide access to all test teams so that they can review, use, and input these test data to meet their objectives. This should enable the use of sequential testing, big data analytics, and other adaptive methods in support of T&E efficiencies. Throughout system development, T&E should be building a shared body of test evidence to support efficient technical, functional, and operational performance evaluations and adaptive T&E. Relevant test data gathered through all testing should be added to this shared data repository. To enable adequate use of sequential testing and similar T&E planning and analysis methods, the T&E WIPT should leverage existing or develop collaborative test data scoring boards to assess test data collected across all phases of the MCA Pathway for potential to meet IOT&E or LFT&E requirements. The OTA should maintain the authoritative record of data collected in IT that has been assessed and authenticated for use in the operational evaluation.

8) **Projected and actual level of funding**

Pursuant to Section 839(b) of Public Law 115-91, the PM should include a table in the TEMP that lists the initial resource estimates for government DT&E, OT&E, and LFT&E, and update this table each time the TEMP is updated. T&E funding in the resources section should be consistent with the cost estimate and budget submissions.

1.5.2 T&E Content and Interests in Other Planning Documents

While the TEMP is the main testing document deliverable during the each of the five major phases of the MCA Pathway, the success of T&E relies heavily on each of the other documents outlined in Table.

a. Capability Development Document (CDD)

The T&E WIPT should be involved with CDD development early to fully understand the desired capabilities and inform how certain system design requirements such as cybersecurity will be evaluated. The test teams should work with their engineering

counterparts to assist in developing requirements that are clear, testable, and measurable, and that requirements traceability exists from the requirements to the test events. Test teams should:

- Understand what constitutes mission effectiveness, suitability, and survivability, and how they will be measured at various acquisition decisions
- Ensure cyber and interoperability needs are clearly defined in the CDD

b. Acquisition Strategy

The Acquisition Strategy should describe the development program and associated decisions sufficiently to convey what information/data testing is needed to adequately support the acquisition decisions and evaluate technical, functional, and operational performance. It should account for T&E when identifying resource needs. The Acquisition Strategy sets the schedule for delivering the capability during the major acquisition phases. Test teams should:

- Ensure thorough description of T&E requirements and data to be provided by the contractor
- Ensure that time is allotted in the program schedule for independent government T&E and time to fix the identified deficiencies
- Ensure that the Acquisition Strategy considers a robust T&E program
- Understand the decision points that will require test data to make informed decisions

c. Systems Engineering Plan (SEP)

Test and Evaluation is a critical element of overall Systems Engineering. T&E provides the means for verifying that product solutions obtained through Systems Engineering Technical Processes will satisfy their design-to requirements and validating that the overall system can meet its stakeholder's capability needs. T&E personnel perform key activities related to Systems Engineering by participating in Technical Assessments and Technical Design Reviews. Such reviews and the assessments that result from them are one of the keys to a knowledge-based acquisition process. The Technical Readiness Assessments (TRA), Preliminary Design Reviews (PDR) and Critical Design Reviews (CDR) provide a venue to establish the technical baselines, assess the system's technical maturity, and review and assess technical risks. Independent Technical Risk Assessments (ITRA) provide an overview of a program's technical risk posture and identifies risks to be brought to the MDA's attention and provide recommended mitigation strategies for high-risk areas.

The SEP documents key technical risks, processes, resources, metrics (Technical Performance Measurement and other metrics), systems engineering (SE) products, quality control, and completed or scheduled SE activities. The purpose of the SEP is to help PMs develop, communicate, and manage the overall SE approach guiding all technical activities of the program. T&E personnel use the SEP as a reference for developing the T&E strategy, test plans, and other planning documents.

d. Validated Online Life Cycle Threat (VOLT)

The VOLT is the authoritative, system-specific threat assessment tailored for and normally focused on one specific program. The VOLT involves the application of threat modules and is written to articulate the relevance of each module to a specific acquisition program or planned capability. While VOLT reports support Acquisition Category (ACAT) I-III programs, only Major Defense Acquisition Programs (MDAPs) and programs on the T&E Oversight List require a unique, system-specific VOLT report to support capability development.

T&E personnel use the VOLT as a reference for developing T&E plans, T&E resources and capability requirements, and test scenarios, as well as a guide for defining the threat environment for a mission-oriented context.

e. Intellectual Property (IP) Strategy

The IP Strategy should identify and describe the management of delivery and associated license rights for all hardware, software, and related materials necessary to meet operational, cyber, and supportability requirements. It should include, to the maximum extent practicable, negotiation for and periodic delivery of all executables, source code, associated scripts, build procedures, automation scripts, tools, databases, libraries, test results, data sets, firmware, training materials, and any other elements necessary to integrate, test and evaluate, debug, deploy, and operate the hardware and software application in all relevant environments (e.g., development, staging, and production). Where third-party services, particularly cloud hosting services, are used, the PM should assure that appropriate access and IP clauses are flowed down to those service providers.

Test teams should provide input to the IP Strategy on the rights to data generated (such as contractor-generated test results) during all phases of testing that would allow building a shared body of test evidence, available to the program throughout its lifecycle. The PM should further consult with the T&E community to determine any access needed to support independent testing and include these accesses in the IP Strategy as needed.

f. Cost Estimate

The cost estimate should consider the technical content of the program described in the CDD, Acquisition Strategy, and TEMP. Test teams should:

- Ensure that the cost estimate includes all the resources necessary to plan and execute the T&E as outlined in the TEMP and resources to mitigate potential deficiencies identified in test

g. Request for Proposal (RFP)

The RFP defines what the government expects from the contractor. If T&E expectations are not explicitly stated in the RFP and the acquisition contract, needed data may not be provided, increasing risk to the T&E program, and potentially, the acquisition cost and schedule. The TEMP is a source document for the RFP and should be generated in time to support RFP development. The PM should consult with government test teams to ensure that the RFP supports data collection for government T&E. At a minimum, a

Service-approved TEMP should be included as an attachment to the RFP to clearly tell the contractors what the government intends to test and evaluate. The test teams should encourage that the following items and activities are included as contract deliverables:

- Government access to contractor test events, test tools, test data repositories, and test environments
- Delivery of contractor-provided M&S tools to be used by government test organizations (these may include initial digital system models, component level reliability and availability models, or other M&S tools)
- Contractor test plans, procedures, reports, and data
- Contractor support for government testing, including early live fire testing

2. T&E During Major Capability Acquisition Pathway Phases

2.1 Materiel Solution Analysis Phase

Specific T&E activities within the Materiel Solution Analysis Phase include:

- Generate the initial Milestone A TEMP[20]
- Actively participate in the development of the RFP for the Technology Maturation and Risk Reduction Phase
- Conduct the Milestone A Independent Technical Risk Assessment (ITRA)
- Supporting the Milestone A decision

2.1.1 Generate the Initial Milestone A TEMP

In coordination with the PM, the T&E WIPT should develop and document the TEMP before progressing to the TMRR phase. The Milestone A TEMP should be complete enough to estimate and plan for the major resources required for adequate T&E in accordance with the requirements outlined in the draft CDD (or ICD), intended use of the system as outlined in CONOPS/OMS/MP, and given the operationally relevant threat as outlined in the VOLT. The Milestone A TEMP should document any risks to the T&E program and describe how the PM will mitigate these risks. To the extent possible, the Milestone A TEMP should:

- Assess the Analysis of Alternatives from the perspective of key drivers of system performance warranting evaluation focus, and key drivers of developmental risk warranting early DT focus
- Present an IDSK that links data requirements for DT&E, OT&E, and LFT&E to key program decisions
- Describe the evaluation focus areas and evaluation framework to meet DT&E, OT&E, and LFT&E
- Present an integrated program schedule that documents major program milestones, and test events supporting those milestones
- Describe each test phase or event
- Identify Milestone entrance and exit criteria
- Identify key T&E resources for the TMRR phase, and their funding
- Highlight any aspects of the CONOPS/OMS/MP that may require significant test assets, such as specialized units, target sets, ranges, threat emulators, threat models and simulations, intelligence mission data, or long production lead times
- If applicable, specify the baseline against which the new system will be judged and the resources allocated for the baseline testing
- Identify key responsible T&E stakeholders, to include stakeholders responsible for verification and validation of proposed M&S and digital tools

[20] In some cases, a T&E strategy may be more appropriate at this phase in the program lifecycle.

2.1.2 Actively Participate in the Development of the RFP for TMRR Phase

The Milestone A TEMP and the approved Acquisition Strategy inform development of the RFPs for any TMRR Phase contracts. The PM, in coordination with the T&E WIPT, should work to ensure that the RFP describes:

- T&E requirements/information needed for a successful T&E program
- T&E data management including T&E data rights
- M&S details, to include pertinent verification, validation, and accreditation (VV&A) reports or plans, if available
- T&E resources
- Cyber contract guidance
- Software management
- Reliability, availability, and maintainability program requirements, including contractual design-for-reliability requirements

The Contract Data Requirements List (CDRL) should identify: 1) required contractor-generated test data, 2) planned contractor T&E objectives and schedules, 3) M&S details, to include capabilities and limitations to be used by the contractor, 4) verification and validation procedures, 5) planned contractor test facility acquisitions, 6) other system information needed to support an adequate T&E, and 7) test assets needed for early live fire testing.

2.1.3 Conduct the Milestone A Independent Technical Risk Assessment (ITRA)

Since 2017, independent technical risk assessments (ITRAs) are required on MDAPs before approval of Milestone A, Milestone B, and any decision to enter into low-rate initial production or full-rate production. T&E professionals are integral ITRA team members. The Milestone A ITRA provides senior leaders with an independent view of program technical risk, including the maturity of critical technologies and manufacturing processes that need to be matured. Specific guidance on the responsibilities and criteria for conducting ITRAs can be found in DoDI 5000.88, Engineering of Defense Systems.

2.2 Technology Maturation and Risk Reduction (TMRR) Phase

Government T&E activities within the Technology Maturation and Risk Reduction Phase include:

- Generate the Milestone B TEMP
- Review the Logistics Risk Assessment
- Conduct the Technology Readiness Assessment
- Participate in the Preliminary Design Review
- Observe or participate in prototype demonstrations or tests
- Participate in the System Requirement and System Functional Reviews
- Participate in the Capability Development Document (CDD) Validation
- Conduct the DT&E Developmental RFP Release Program Assessment (DTA)
- Conduct the Milestone B Independent Technical Risk Assessment (ITRA)
- Conduct the Milestone B DT&E Sufficiency Assessment (DTSA)
- Conduct an early operational assessment, if applicable

- Support the Development RFP Release Decision for the EMD Phase
- Support the Milestone B decision

2.2.1 Generate the Milestone B TEMP

The Milestone B TEMP should expand on and update the Milestone A TEMP content. For example, the Milestone B TEMP should:

- Adapt the IDSK, the evaluation framework, and associated fidelity of test and M&S events, to include verification and validation to leverage and build on the contractor and government testing, M&S, and analysis conducted in the previous phase
- Include the IOT&E design completed by the OTA to define operational test requirements and support test resource estimates
- If applicable, commit to FUSL live fire testing, or the Program Office, in coordination with the T&E WIPT, should submit a FUSL waiver request and detail the alternative LFT&E strategy in the TEMP in accordance with Title 10, Section 4172 USC
- Update the estimates of test risks that may prevent or delay the satisfactory execution of the test events
- Discuss safe test procedures and adequate environmental protections
- Update the projected resource and schedule requirements, including simulated threat environments and targets

2.2.2 Review the Logistics Risk Assessment

The Logistics Risk Assessment is an analysis of a program's product support strategy across the system lifecycle, including sustainment costs. The T&E WIPT should review the logistics risk assessment and leverage it during development of the Milestone B TEMP.

2.2.3 Conduct the Technology Readiness Assessment (TRA)

The TRA is a systematic, metrics-based process that assesses the maturity of, and the risk associated with, critical technologies to be used in MDAPs. The assessment should be based on objective evidence gathered during events, such as tests, demonstrations, pilots, or physics-based simulations. Program Managers conduct TRAs with the assistance of an independent team of subject matter experts that can include T&E professionals. For programs for which an ITRA is conducted, a technology readiness assessment report is not required as the ITRA report subsumes the TRA findings. Programs will continue to assess and document the technology maturity of all critical technologies consistent with the USD(R&E) technology readiness assessment guidance.

2.2.4 Participate in Preliminary Design Review (PDR)

The PDR is the first opportunity for T&E professionals to closely observe the contractor's hardware and software design. The PDR occurs after preliminary system design efforts but before drafting the detailed system designs. During the PDR, the

contractor describes the rationale for the system's preliminary design, outlining all the designs considered, changes that were made as a result of trade studies, and the resulting design decisions.

2.2.5 Conduct the DT&E Developmental RFP Release and Milestone B Program Assessment (DTA)

The USD(R&E) provides the MDA with a program assessment at the development RFP release decision point and Milestone B. These programs, if designated for DT oversight by the USD(R&E), can include MDAPs, other programs categorized as ACAT I; major systems, usually categorized as ACAT II; automated information systems (AIS) (not managed by other acquisition pathways); and other capabilities developed via the MCA Pathway. The Developmental RFP assessment reviews the overall proposed RFP and the Contract Data Requirement List for inclusion of T&E execution support. The assessment will address the adequacy of the proposed approach on T&E technical data, including management, ownership, control, timely access, and delivery of the T&E data, to include raw test data, to support future program development. Given the early maturity of the program at this stage with minimal test data available, the DT&E Milestone B program assessment focuses on the adequacy of planned testing for evaluating technical performance and technology, demonstrated capabilities, integration maturity, sustainment, and survivability.

2.2.6 Conduct the Milestone B Independent Technical Risk Assessment (ITRA)

The Milestone B ITRA considers the full spectrum of technology, engineering, and integration risk. These areas could include mission capability, technology, system development, MOSA, software, security, manufacturing, sustainment, testing adequacy, and their potential impacts to cost, schedule, and performance. Specific guidance on the responsibilities and criteria for conducting ITRAs can be found in DoDI 5000.88, Engineering of Defense Systems

2.2.7 Conduct the Milestone B DT&A Sufficiency Assessment (DTSA)

In accordance with 10 U.S.C. §4252, when the USD(A&S) is the MDA, the USD(R&E) will conduct DT&E sufficiency assessments for MDAPs. Milestone B DT&E sufficiency assessments will include a focus on reliability, interoperability, and cybersecurity, concentrating on the adequacy of planned testing. The assessment will address the sufficiency of:

- The DT&E plans within the TEMP
- The DT&E schedule, including a comparison to historic, analogous systems
- The DT&E resources (facilities, personnel, test assets, data analytics tools, and M&S capabilities)
- The mitigation of known risks of developmental test and production concurrency
- The developmental test criteria for entering the production phase

Findings should be included in the Milestone B brief summary report provided to the congressional defense committees. When the Service or the Component acquisition

executive is the MDA, the senior official within the Military Department, Defense Agency or DoD Field Activity with responsibility for DT&E will conduct the Milestone B Sufficiency Assessments and report the results to the congressional defense committees. An example of the Milestone B DT&E sufficiency assessment is at Appendix B.

2.2.8 Conduct an Early Operational Assessment (EOA)

EOAs and relevant live fire testing should be conducted to provide a means to evaluate a program's progress early in the process toward developing an operationally effective, suitable, survivable, and lethal system. An EOA is conducted in accordance with a test plan approved by DOT&E for programs under T&E oversight. EOAs are typically an analysis, based on a review of current program plans and documentation, as well as data from early developmental testing, technology assessments, M&S, and program reviews, to include PDR. EOAs enable the OTA to provide early input on key operational strengths and risks inherent to the design that, if not corrected, could have a detrimental effect on the determination of operational effectiveness, suitability, survivability, and lethality. EOAs examine the links and consistency between the concept of operations, requirements, and technology limitations to provide recommendations to the program and the requirements authority. DOT&E (when applicable), and the appropriate OTA should report EOA findings to their Service Chief and the MDA to support the Milestone B decision.

2.2.9 Support the Development of RFP Release Decision for the EMD Phase

The Development RFP Release Decision commits the program to releasing the Development RFP to industry. The Development RFP Release Decision should be based on the program's executability and affordability prior to releasing the EMD solicitation. The goal is to avoid any major program delays at Milestone B, when source selection is already complete and award is imminent. At the Development RFP Release Decision, the PM provides a draft Milestone B TEMP for the EMD Phase. The T&E WIPT also assists in developing the RFP to ensure it addresses:

- Government T&E requirements identified in the Milestone B TEMP
- Contractor T&E activities critical for program success

2.3 Engineering and Manufacturing Development (EMD) Phase

Government T&E activities within the EMD Phase include:

- Generate the Milestone C TEMP
- Participate in the Critical Design Review
- Conduct Government T&E
  - Conduct DT&E on Components, Subsystems, and Prototype Systems
  - Conduct Operational Assessment(s)
  - Live Fire T&E Activities
- Support the Production & Deployment RFP Release
- Conduct the Milestone C DT&E Program Assessment

- Conduct the Low-Rate Initial Production (LRIP) Independent Technical Risk Assessment (ITRA)
- Conduct the Milestone C DT&E Sufficiency Assessment
- Support Milestone C and LRIP decisions

2.3.1 Generate the Milestone C TEMP

The Milestone C TEMP should expand on and update the Milestone B TEMP content. For example, the Milestone C T&E TEMP should:

- Adapt the IDSK, the evaluation framework, and the fidelity of test and M&S events, to include VV&A, to leverage and build on the contractor and government testing, M&S, and analysis conducted in the previous phase
- Detail the Initial Operational Test & Evaluation (IOT&E), which is required by 10 U.S.C. § 4171 and all other planned data collection events
- Detail the LFT&E Full-Up System-Level (FUSL) testing, required by 10 U.S.C. § 4172
- Update the estimates of test risks that may prevent or delay the satisfactory execution of the test events
- Update the projected resource and schedule requirements, including simulated threat environments and targets

Delays in system development can pose a schedule risk for T&E activities. If the PM decides to compress the T&E activities laid out in the integrated program schedule within the TEMP, testers should characterize the risk of failing to obtain the information detailed in the developmental and operational evaluation frameworks and the LFT&E Strategy.

2.3.2 Participate in the Critical Design Review (CDR)

The CDR is the decision point for certifying the system design has sufficiently matured for hardware fabrication to begin with acceptable risk. The T&E WIPT representatives should attend the CDR and provide an up-to-date assessment of the system. In particular, the CDR assesses design maturity, documentation, and risks, and establishes the initial system baseline.

2.3.3 Conduct Government T&E

2.3.3.1 Conduct Government DT&E on Components, Subsystems, and Prototype Systems

Government testers should continue to leverage contractor testing when appropriate to supplement government DT&E. Programs are encouraged to include military users in government-conducted DT&E to support early problem identification and user acceptance. Involving users in government-conducted DT&E also encourages integrated T&E activities by increasing the relevance of the data to the OT&E stakeholders.

2.3.3.2 Conduct Operational Assessment(s)

OTAs typically execute one or more operational assessments (OA) during the EMD Phase to provide timely and frequent feedback on capabilities as they are developed during this phase. The data for OAs may include multiple test events (DT, IT, and OT) and data analysis efforts conducted before initial production units are available and which incorporates substantial operational realism. OAs may include evaluations that range from operational analysis of system designs to assess potential design operational strengths or risks to test events that include military users with varying degrees of operational missions' realism based on the level of system maturity. An OA may be combined with developmental test activity and/or training events. The lead OTA conducts an OA in accordance with a test plan approved by DOT&E for programs under T&E oversight. As a general criterion for proceeding through Milestone C, the lead OTA will conduct and report results of at least one OA. The OTA supports the Milestone C decision by reporting the findings of any relevant DT, IT, and OT&E conducted to date. The OTA Report should focus on progress toward operational effectiveness, suitability, survivability, and lethality and any associated risks. The OTA report should also include an assessment of significant trends noted in development efforts, adequacy of performance against operational and technical requirements, and the program's ability to support adequate operational testing.

2.3.3.3 Live Fire T&E Activities

LFT&E can generate information supporting the evaluation of a system's operational effectiveness, suitability, survivability and lethality. The DOT&E approves LFT&E strategies and LFT&E test plans (including survivability and lethality test plans) for covered systems as defined in Section 4172 of Title 10, U.S.C., as well as the quantity of test articles procured for all LFT&E test events for any system under LFT&E oversight. LFT&E occurs over the course of a program, beginning with component-level testing during the initial design stage. T&E continues as the system matures from assemblies to sub-systems, and finally, unless waived, to FUSL configuration. During FUSL testing, the weapon system is fully equipped for combat with all sub-systems operational and powered. Survivability and lethality tests should be carried out sufficiently early in the development phase of the system or program to allow for the correction of design deficiencies discovered during testing before proceeding beyond low-rate initial production.

Although there is no waiver from LFT&E, the law contains provisions for a waiver from the requirements for FUSL testing. The Program Executive Officer will provide a memorandum to the Service Acquisition Executive asserting that the survivability or lethality tests required by 10 USC 4172 are unreasonably expensive and impractical. The SAE will provide a similar memorandum to USD(A&S) as the Defense Acquisition Executive requesting a waiver from the requirement of FUSL testing on that basis. The waiver must be approved by USD(A&S) as the DAE, even in cases where acquisition authority has been delegated to the Service.

USD(A&S) will request that DOT&E certify that the live fire testing and evaluation laid out in the TEMP (or previously in the Live Fire Strategy/Alternative Live Fire Test and Evaluation Plan) is adequate to evaluate the survivability or lethality of the system

without using FUSL assets. DOT&E will provide a memorandum affirming this to be the case, along with the approved TEMP (or the appropriate live fire sections of the TEMP) to USD(A&S). In accordance with 10 USC 4172 (c)(3), USD(A&S) will then submit memoranda and the live fire plan to the chairs and ranking members of the congressional defense committees, informing them of the granting of the waiver.

The waiver package sent to Congress consists of these two parts: 1) certification that the waiver is needed and 2) an LFT&E plan for evaluating survivability or lethality.

2.3.4 Support the Production and Deployment RFP Release

Given the maturity of the program at this stage in the acquisition cycle, programs may need to update the RFP. The updated RFP may include changes to T&E requirements, but should be consistent with the Milestone C TEMP and the Acquisition Strategy.

2.3.5 Conduct the Milestone C DT&E Program Assessment (DTA)

The USD(R&E) provides the MDA with an assessment to inform the Milestone C decision for those programs designated for DT oversight. These can include MDAPs, other programs categorized as ACAT I; major systems, usually categorized as ACAT II; automated information systems (AIS) (not managed by other acquisition pathways); and other capabilities developed via the MCA Pathway. The USD(R&E) uses all available test data to evaluate technical performance and technology, demonstrated capabilities, integration maturity, sustainment, and survivability. The USD(R&E) coordinates with the Director, Operational Test and Evaluation on the integration of developmental and operational test and evaluation to minimize duplicative testing and reporting to the maximum extent possible and achieve greater efficiencies.

2.3.6 Conduct the Low-Rate Initial Production (LRIP) Independent Technical Risk Assessment (ITRA)

An ITRA is required for MDAPs before approval of any decision to enter into LRIP. The LRIP ITRA assessment areas include mission capability, technology, system development, MOSA, software, security, manufacturing, sustainment, testing adequacy in, and their potential impacts to program cost, schedule, and performance. Specific guidance on the responsibilities and criteria for conducting ITRAs can be found in DoDI 5000.88, Engineering of Defense Systems.

2.3.7 Conduct the Milestone C DT&E Sufficiency Assessment (DTSA)

In accordance with 10 U.S.C. §4253 when the USD(A&S) is the MDA, the USD(R&E) will conduct a DTSA to support the Milestone C decision and entry into the P&D Phase for MDAPs. The Milestone C DTSA focuses on the sufficiency of completed testing, the risks identified during that testing, and the plans for remaining testing. The reportable elements that the USD(R&E) provides to the USD(A&S) for inclusion in their Milestone C Brief Summary Report submitted to the congressional defense committees are:

- DT&E completed
- DT&E Plans (for remaining DT&E)

- Risks to Production and Deployment
- DT&E Resources (for remaining DT&E)
- Readiness for IOT&E

When the Service or the Component acquisition executive is the MDA, the senior official within the Military Department, Defense Agency, or DoD Field Activity with responsibility for DT&E will conduct and report the DTSA results to the MDA for their Milestone C Brief Summary Report to the congressional defense committees.

2.3.8 Support the Production and Deployment RFP Release

Given the maturity of the program at this stage in the acquisition cycle, programs may need to update the RFP. The updated RFP may include changes to T&E requirements, but should be consistent with the Milestone C TEMP and the Acquisition Strategy.

2.4 Production and Deployment Phase

Government T&E activities within the Production and Deployment Phase include:

- Generate the Full-Rate Production (FRP) TEMP, as necessary
- Conduct Government T&E, to include any remaining DT&E and LFT&E (e.g., FUSL Testing if applicable), IOT&E
- Generate an IOT&E Report
- Conduct the FRP Independent Technical Risk Assessment (ITRA)

2.4.1 Generate the Full-Rate Production TEMP

At any point after the FRP or full deployment decision, DOT&E and/or Director, DTE&A may direct the DoD Component Acquisition Executive (CAE) to provide TEMP updates or addendums to articulate additional testing (e.g., FOT&E, Verification of Correction of Deficiencies periods, or test programs for future increments). The OTA may also request TEMP updates or addendums to articulate additional testing.

2.4.2 Conduct Government T&E

2.4.2.1 First Article Testing (FAT):

The purpose of FAT is to evaluate how production processes and environmental stress affect system performance. FAT should be conducted expeditiously because the production line may continue to flow while testing is conducted and results are being analyzed.

2.4.2.2 Acceptance Testing (AT):

The purpose of AT is to ensure that each system that comes off the production line functions properly. AT is critical because it is the point where the government accepts ownership and responsibility of the system, and may also be the date on which warranty coverage begins.

Both FAT and AT are normally conducted either by Program Management Office personnel or by the contractor using government-approved test plans and under the oversight of government personnel resident at the contractor facility.

2.4.2.3 Production Qualification Tests (PQT):

PQT is conducted post-Milestone C to ensure the effectiveness of the manufacturing process, equipment, and procedures, and provides data for the independent evaluation required for materiel release so that the evaluator can address the adequacy of the materiel with respect to the stated requirements. These tests are conducted on a number of samples taken at random from the first production lot. PQT is repeated if the process or design is changed significantly and when a second or alternative source is brought on line.

2.4.2.4 Initial Operational Test and Evaluation (IOT&E):

An IOT&E, a test event mandated by 10 U.S.C. § 4171, provides Congress, the Secretary of Defense, the Milestone Decision Authority, and the warfighter an independent evaluation of a system's operational effectiveness, suitability, survivability, and lethality. The lead OTA conducts an IOT&E in accordance with a test plan approved by the DOT&E for programs under OT & LFT&E oversight.

IOT&E uses production or production-representative test articles that, at a minimum, will incorporate the same materials and processes, including system parts and software items, to be used in production articles. Properly qualified integrated test data collected during EMD may be used to fulfill some IOT&E requirements subject to DOT&E approval or the OTA approval in the absence of DOT&E oversight. IOT&E also requires more than an evaluation based exclusively on computer modeling, simulation, or an analysis of system requirements, engineering proposals, design specifications, or any other information contained in program documents. It requires end-to-end testing of system capabilities, including all interrelated systems needed to employ and support those capabilities when operated by typical (trained) users or units under conditions simulating combat stress, or if applicable, peacetime operations. Individuals employed by the contractor for the system being developed may only participate in IOT&E to the extent they are planned to be involved in the operation, maintenance, and other support of the system when deployed in combat.

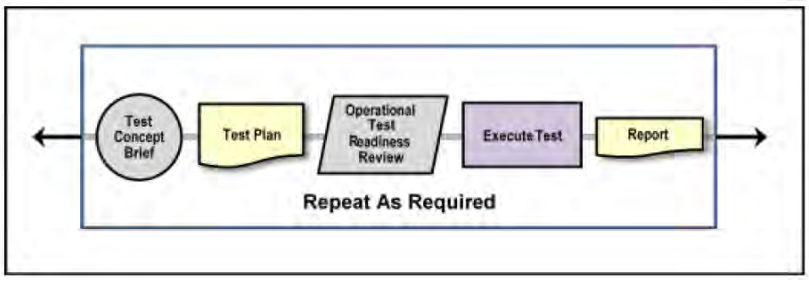


Figure 4. Typical sequence of OT&E activities

2.4.2.5 Full-Up System-Level (FUSL) Tests

FUSL testing fulfills the requirements of Title 10, U.S.C. Section 4172 for "realistic survivability" and "realistic lethality" testing. "Realistic survivability testing" means testing for the susceptibility, vulnerability, force protection, and recoverability of the system and its crew in a contested operational environment using adversary-

representative threats fired against the production-representative system equipped with any available countermeasures. “Realistic lethality testing” means testing for lethality by engaging the production-representative weapon against adversary-representative targets configured for combat equipped with any associated countermeasures.

DOT&E approves LFT&E plans for select live fire test events, as identified in the TEMP. Examples include FUSL tests, Total Ship Survivability Trials, Full Ship Shock Trials, M&S plans, and similar. The document approval matrix in the TEMP specifies which planning documents will be submitted for DOT&E approval and which will be submitted for information and review only. The Service OTA or assigned test activity conducts LFT&E events, executing the planned events in accordance with the LFT&E strategy and approved LFT&E plan.

2.4.3 Generate an IOT&E Report

For programs on OT or LFT&E oversight, DOT&E issues an IOT&E report to the MDA, Secretary of Defense, and Congress. The report includes the Director’s independent assessment of test adequacy and an evaluation of the system’s operational effectiveness, suitability, survivability, and lethality. For programs on the T&E Oversight List, operational and live fire testing occurs in accordance with the DOT&E-approved TEMP and subsequent operational test and LFT&E plans. For programs only on LFT&E oversight, the Director will submit a report at the conclusion of survivability or lethality testing.

If a decision is made to proceed to operational use or make procurement funds available prior to the completion of IOT&E, DOT&E will submit a report to the Secretary of Defense as soon as practicable, referred to as an Early Fielding report. An Early Fielding report will document test adequacy and provide an assessment of operational effectiveness, suitability, survivability, and lethality.

2.4.4 Conduct the Full-Rate Production Independent Technical Risk Assessment (ITRA)

An ITRA is required for MDAPs before approval of any decision to enter into Full-Rate Production (FRP). The FRP ITRA assessment areas include demonstrated mission capability, technology, system development, MOSA, software, security, manufacturing, sustainment, testing adequacy and their potential impacts to program cost, schedule, and performance. Specific guidance on the responsibilities and criteria for conducting ITRAs can be found in DoDI 5000.88, Engineering of Defense Systems.

2.5 Operations and Support (O&S) Phase

Government T&E activities within the Operations and Support Phase does not end upon full-rate decision. The O&S phase focuses on executing the product support strategy, satisfying materiel readiness and operational performance requirements, and sustaining the system. Effective sustainment of systems results from the design and development of supportable, reliable, and maintainable systems. Sustainment strategies can evolve throughout the system’s life cycle. The PM works with system users to document performance and sustainment requirements in agreements specifying objective outcomes,

measures, resource commitments, and stakeholder responsibilities. The Services, with system users, conduct continuing reviews of sustainment strategies to compare performance expectations against actual performance measures. When appropriate, follow-on activities include planning for a Follow-on Operational Test & Evaluation (FOT&E) conducted by the OTA's to evaluate operationally significant improvements, modifications, and corrective actions made to the system subsequent to the IOT&E. Surveillance testing and shelf-life extension testing.

2.5.1 Follow-on Operational Test & Evaluation (FOT&E)

An FOT&E is a test event that may be conducted, if necessary, after IOT&E to determine whether deficiencies identified during IOT&E were corrected, or to evaluate aspects of system performance not tested during IOT&E due to test or system limitations or because system updates were required. An FOT&E is conducted in accordance with a DOT&E-approved test plan for systems on T&E oversight. FOT&E should be conducted in a realistic tactical environment similar to IOT&E and use production systems with appropriate modifications, upgrades, or increments. FOT&E verifies and evaluates the operational effectiveness, suitability, survivability, and lethality of the production system in light of any changes to the system or operational environment. Additional FOT&E may be conducted over the life of the system to refine doctrine, tactics, techniques, and training programs, and to evaluate future increments, modifications, and upgrades. Specific objectives of FOT&E include testing modifications to be incorporated into production systems. The tests are also used to evaluate the system in a different platform application for new tactical applications or against new threats.

Appendix A. Acronyms & Glossary

ACAT	Acquisition Category
AT	Acceptance Testing
BLRIP	Beyond Low-Rate Initial Production
CDRL	Contract Data Requirements List
CDD	Capability Development Document
CDR	Critical Design Review
CDT	Chief Developmental Tester
COI	Critical Operational Issue
CONOPS	Concept of Operations
CTP	Critical Technical Parameter
DEF	Developmental Evaluation Framework
DOT&E	Director, Operational Test and Evaluation
DSQ	Decision Support Question
DTA	Developmental Test Assessment
DT&E	Developmental Test and Evaluation
D,DTE&A	Director, Developmental Test and Evaluation
DTSA	Developmental Test Sufficiency Assessment
EMD	Engineering and Manufacturing Development
EOA	Early Operational Assessment
FAT	First Article Testing
FD	Full Deployment
FOT&E	Follow-on Operational Test and Evaluation
FRP	Full-Rate Production
FUSL	Full-Up System-Level
ICD	Initial Capabilities Document

IDSK	Integrated Decision Support Key
IOT&E	Initial Operational Test and Evaluation
ITRA	Independent Technical Risk Assessment
JMETC	Joint Mission Environment Test Capability
KPP	Key Performance Parameter
KSA	Key System Attribute
LFT&E	Live Fire Test and Evaluation
LRIP	Low-Rate Initial Production
LVC	Live, Virtual, or Constructive
M&S	Modeling and Simulation
MCA	Major Capability Acquisition
MCF	Mission Critical Function
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MP	Mission Profile
MRTFB	Major Range and Test Facility Base
MSA	Material Solution and Analysis
O&S	Operations and Support
OA	Operational Assessment
OEF	Operational Evaluation Framework
OMS	Operational Mode Summary
OPM	Operational Performance Measure
OT&E	Operational Test and Evaluation
OTA	Operational Test Agent
OTP	Operational Test Plan
P&D	Production and Deployment
PDR	Preliminary Design Review

PM	Program Manager
RFP	Request for Proposals
T&E	Test and evaluation
TBPM	Technical Baseline Performance Measure
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction
TPM	Technical Performance Measure
TRA	Technology Readiness Assessment
VV&A	Verify, Validate, and Accredit
VOLT	Validated Online Lifecycle Threat
WIPT	Working-level Integrated Product Team

Appendix B. DT&E Sufficiency Assessment Memorandum Examples

Milestone B DT&E Sufficiency Assessment Memorandum Example

[OFFICE LETTERHEAD]

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT [OR COMPONENT/SERVICE ACQUISITION EXECUTIVE]

SUBJECT: Developmental Test and Evaluation Sufficiency Assessment for the <*name of program*> Program in Support of the Milestone B Brief Summary Report

This memorandum provides my assessment of the sufficiency of developmental test and evaluation (DT&E) plans for the <*name of program*> program as required by section 2366b(c)(1)(G) of Title 10, United States Code.

I have conducted a formal review of the program's DT&E efforts and, on the basis of such review, assess that the DT&E is <*sufficient*><*not sufficient*> to support Milestone B and entry into the Engineering and Manufacturing Development (EMD) phase. During my review and assessment, I have determined the following:

DT&E Planning. The DT&E plans within the Test and Evaluation Master Plan are <*sufficient*><*not sufficient*> to support the EMD phase.

Basis for Assessment. *Provide a brief discussion supporting assessment of DT&E planning. Summarize DT&E planning concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

DT&E Schedule. The DT&E integrated master schedule for EMD is <*sufficient*><*not sufficient*>.

Basis for Assessment. *Provide a brief discussion supporting assessment of the DT&E schedule. Summarize DT&E schedule concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

DT&E Resources. The planned DT&E resources (including facilities, personnel, test assets, automated data analytics tools, and modeling and simulation capabilities) supporting EMD are <*sufficient*><*not sufficient*>.

Basis for Assessment. *Provide a brief discussion supporting assessment of DT&E resources. Summarize DT&E resource planning concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

Risks of Developmental Test and Production Concurrency. The mitigation of known risks of developmental test and production concurrency is <*sufficient*><*not sufficient*>.

Basis for Assessment. *Provide a brief discussion identifying DT&E risks and supporting DT&E risk mitigation. Summarize DT&E risk concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

DT&E Entrance Criteria for Production Phase. The developmental test criteria for entering the production phase are <*sufficient*><*not sufficient*>.

Basis for Assessment. *Provide a brief discussion supporting DT&E production phase entrance criteria. Summarize DT&E entrance criteria concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

Additional Information (optional). *Provide the MDA with any relevant information (e.g. Supply Chain Security) appropriate to this DT&E sufficiency assessment. Use an attachment, if necessary.*

The point of contact for additional details and analysis supporting this DT&E sufficiency assessment is <*Name, Email Address, and Phone Number*>.

<*Signature block of the D(DTE&A)*> *or*

<*Signature block of senior official within the Military Department, Defense Agency, or DoD Field Activity with responsibility for DT&E* >

cc:

USD(R&E) or DD(Engineering) if Component signed
DOT&E

Milestone C DT&E Sufficiency Assessment Memorandum Example

[OFFICE LETTERHEAD]

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT [OR COMPONENT/SERVICE ACQUISITION EXECUTIVE]

SUBJECT: Developmental Test and Evaluation Sufficiency Assessment for the <*name of program*> Program in Support of the Milestone C Brief Summary Report

This memorandum provides my assessment of the sufficiency of developmental test and evaluation (DT&E) completed for the <*name of program*> program as required by section 2366c(a)(4) of Title 10, United States Code.

I have conducted a formal review of the program's completed DT&E and assess on the basis of such review that the DT&E completed is <*sufficient*><*not sufficient*> to support Milestone C and entry into the Production and Deployment (P&D) phase. During my review and assessment, I have determined the following:

Completed DT&E. The evaluation of results from DT&E completed to date is <*sufficient*><*not sufficient*> to support entry into the P&D phase.

Basis for Assessment. *Provide a brief discussion supporting assessment of completed DT&E. Summarize DT&E completion concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

DT&E Remaining Plans and Resources. The plans and resources available for remaining DT&E are <*sufficient*><*not sufficient*> to support the P&D phase.

Basis for Assessment: *Provide a brief discussion supporting assessment of remaining DT&E plans and resources. Summarize DT&E remaining plans and resources concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

Risks to the P&D Phase Identified During DT&E. The mitigation of risks identified during DT&E to the P&D phase is <*sufficient*><*not sufficient*>.

Basis for Assessment. *Provide a brief discussion supporting DT&E risk mitigation. Summarize DT&E risk concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

System Readiness for Initial Operational Test and Evaluation (IOT&E). The system is *<ready/not ready>* for scheduled IOT&E.

Basis for Assessment. *Provide a brief discussion supporting system readiness for IOT&E assessment. Summarize DT&E IOT&E readiness concerns with recommendations to resolve any issues. Use an attachment, if necessary.*

Additional Information (optional). *Provide the MDA with any relevant information (e.g. Supply Chain Security) appropriate to this DT&E sufficiency assessment. Use an attachment, if necessary.*

The point of contact for additional details and analysis supporting this DT&E sufficiency assessment is *<Name, Email Address, and Phone Number>*.

<Signature block of the D(DTE&A)> or

<Signature block of senior official within the Military Department, Defense Agency, or DoD Field Activity with responsibility for DT&E >

cc:

USD(R&E) or DD(Engineering) if Component signed

DOT&E

TEST AND EVALUATION CHAPTER 5: SOFTWARE ACQUISITION

Table of Contents

1. Software Acquisition Pathway Overview

1.1 Introduction

The Software Acquisition Pathway is used for the timely acquisition of software capabilities developed for the DoD. Programs using the Software Acquisition Pathway are required to deliver the first increment of viable and effective capability no later than one year after funds are obligated, after which new capabilities must be delivered to operations at least annually to iteratively meet requirements, but more frequent updates and deliveries are encouraged where practical.[21]

Testing organizations should be involved with the acquisition program early and continually throughout its lifecycle to support effective and efficient evaluations and delivery timelines. Contractor development testing, government developmental testing, system safety assessment, security certifications, and operational test and evaluation should be integrated, streamlined, and automated to the maximum extent practicable to enable rapid analysis of test data and evaluation of system operational effectiveness, suitability, and survivability to inform the decision authorities. Maximum sharing, reciprocity, availability, and reuse of test results and artifacts among testing and certification organizations are necessary for success.

This chapter describes T&E community involvement throughout the Software Acquisition Pathway lifecycle.

1.2 Software Acquisition Pathway Description

There are two paths within the Software Acquisition Pathway: applications and embedded software. This T&E guidance applies to both paths. Unique considerations for the embedded software path are highlighted throughout the document.

- **Applications Path.** Provides for rapid development and deployment[22] of software running on commercial hardware, including modified hardware and cloud computing platforms.[23]
- **Embedded Software Path.** Provides for the rapid development, deployment, and insertion of upgrades and improvements to software embedded in weapon systems and other military-unique hardware systems. The system in which the software is embedded could be acquired via other acquisition pathways (e.g., Major Capability Acquisition).[24]

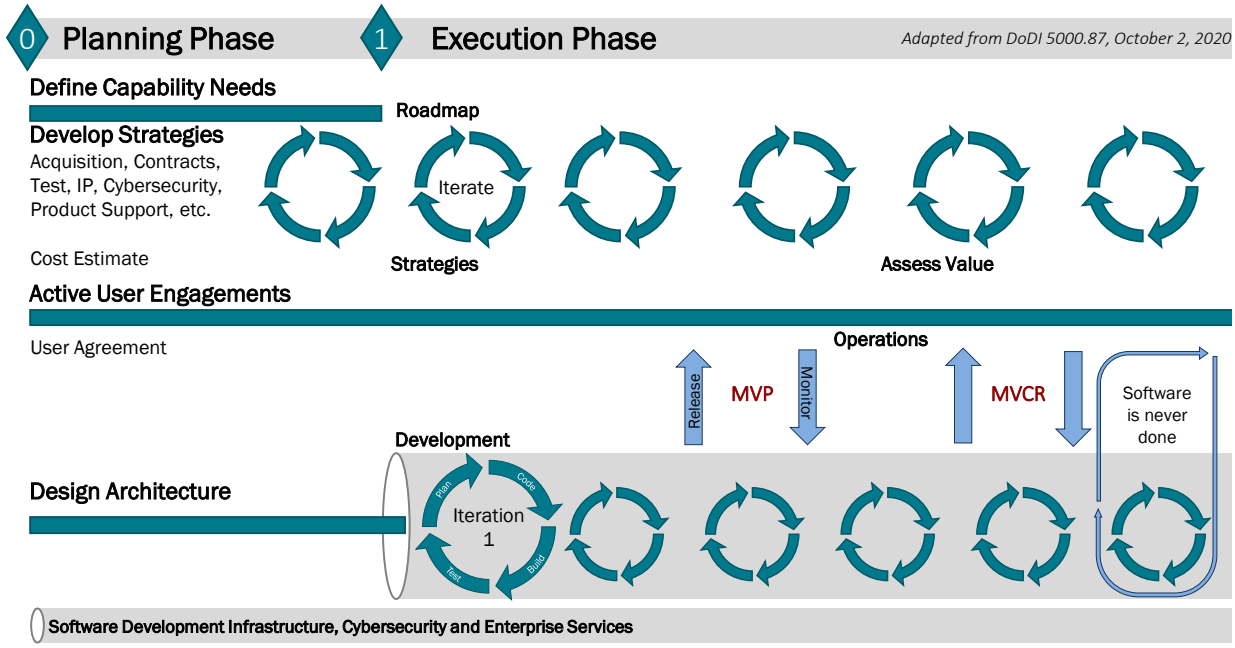
Independent of the path, the Software Acquisition Pathway has two phases: planning and execution, depicted in Figure 1.

[21] DoDI 5000.87

[22] Deployment is when the code reaches the operational users.

[23] DoDI 5000.87

[24] DoDI 5000.87



Acronyms: DoDI – DoD Instruction; IP – Intellectual Property; MVP – Minimum Viable Product; MVCR – Minimum Viable Capability Release

Figure 1. Software Acquisition Pathway

1.2.1 Planning Phase

The purpose of the Planning Phase is to better understand users' needs and plan the approach to deliver software capabilities to meet those needs.[25] As the Planning Phase sets the conditions for success, test teams should be involved early in the program during the Planning Phase to establish and document how testing will be accomplished. Details of T&E Community involvement during the Planning Phase are discussed in Section 2.

1.2.2 Execution Phase

During the Execution Phase, the software is designed, developed, integrated, tested, delivered, deployed, operated, and monitored. Programs will spend the majority of their life cycles in the Execution Phase. Activities during this phase will be guided by the product roadmap, which identifies goals and features of the software.

The Software Acquisition Pathway stresses the concept of iterative development, which includes iterative software development methods (e.g., Agile, DevSecOps) tools, and automation (e.g., automated test scripts). Readers can consult the *DoD Enterprise DevSecOps Fundamentals*[26] published by the DoD Chief Information Officer (CIO) for more information on methods and tools, which provides a compendium of universal concepts related to DevSecOps, as part of a library of guidebooks, playbooks, and reference designs.[27] The DevSecOps library provides deep knowledge and industry best practices that can directly benefit program offices and intermediate

[25] DoDI 5000.87, pg. 9

[26] https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsFundamentals.pdf

[27] Library of documents is available here: https://dodcio.defense.gov/Library/

staff. In particular, there is a document on DevSecOps Tools and Activities that testers should reference for potential use in testing strategies. For additional information on Agile concepts and terms, readers can refer to the DAU Agile 101 Primer[28] and Agile Software Acquisition Guidebook[29].

The iterative process is highlighted through the "Plan, Code, Build, Test" components of each development cycle, as labeled in Iteration 1 of Figure 1. It includes delivering and deploying software in small increments that build on each other.

As shown by the "test" component of each development cycle, testing occurs throughout the iterative development process. This includes contractor testing and independent government testing. For programs using the embedded software path, this testing should be aligned with the system in which the software is embedded. Details of government testing and test team involvement throughout the Execution Phase are discussed in Section 3.

1.2.2.1Minimum Viable Product (MVP)

The MVP is developed during the Execution Phase and is an "early version of the software to deliver or field basic capabilities to the users to evaluate and provide feedback on. Insights from MVPs help shape scope, requirements, and design."[30] Note that the MVP is not intended to be fielded for operational use.

T&E of the MVP is discussed in Section 3.3.1.

1.2.2.2Minimum Viable Capability Release (MVCR)

The MVCR is developed during the Execution Phase and contains "the initial set of features suitable to be fielded to an operational environment that provides value to the warfighter or end user in a rapid timeline."[31] The MVCR delivers initial warfighting capabilities to enhance some mission outcome and is intended to be fielded to an operational environment for operational use.

The MVCR must be deployed to an operational environment within one year after the date on which funds are first obligated to acquire or develop new software capability, including appropriate operational test. If the MVP version of the software is determined sufficient to be fielded for operational use, the MVP may become the MVCR.

T&E of the MVCR is discussed in Section 3.3.2.

1.2.2.3 Value Assessments

During the Execution Phase, "the sponsor"[32] and user community will perform a value assessment at least annually on the software delivered. The sponsor will provide feedback on whether the mission improvements or efficiencies realized from the delivered software

---

[28] https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/Agile%20101%20v1.0.pdf

[29] https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/AgilePilotsGuidebook%20V1.0%2027Feb20.pdf

[30] DoDI 5000.87, Glossary

[31] DoDI 5000.87, Glossary

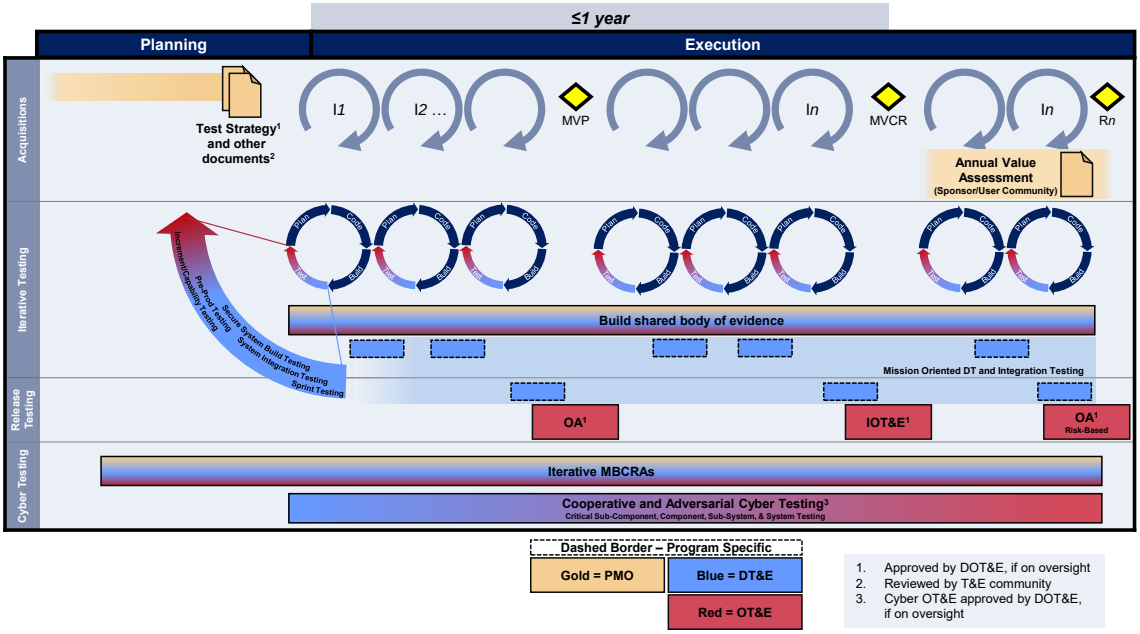
[32] DoDI 5000.87 defines the sponsor as "the individual that holds the authority and advocates for needed end user capabilities and associated resource commitments." This guidance identifies further roles within the sponsor organization.

capabilities are timely and worth the investment. The feedback should be informed by test and evaluation results."[33] Support from T&E for these value assessments is discussed in Section 3.5.

1.3 Software Acquisition Pathway T&E Overview

During the Planning Phase, the test teams should be involved in developing acquisition documents and establishing the testing infrastructure, tools, and data requirements. The T&E Strategy is developed and written during this phase, and approved by DOT&E if on oversight.

During the Execution Phase, contractor and independent government test teams should continuously test and evaluate the software being developed. Figure 2 summarizes how this guidance envisions T&E across the Software Acquisition Pathway. It highlights both testing



activities and evaluation products throughout the acquisition lifecycle. The testing and evaluation shown in this figure is described throughout this chapter. The iterative testing line is described throughout Section 3.2. The release testing line is described in Section 3.3. Cyber testing is briefly described in Section 3.2.6.

Acronyms: DOT&E – Director, Operational Test and Evaluation; T&E – Test and Evaluation; DT&E – Developmental Test and Evaluation; OT&E – Operational Test and Evaluation; OA – Operational Assessment; IOT&E – Initial Operational Test and Evaluation; MBCRA – Mission Based Cyber Risk Assessment

Figure 2. T&E Aligned with Software Acquisition Pathway

1.4 Test and Evaluation Working-level Integrated Product Team (WIPT)

The T&E WIPT coordinates top-level planning for all test events, and assists in the evaluation of test results to support systems engineering and programmatic decision-making.

The T&E WIPT is conducted in an open forum that includes the test and evaluation subject matter experts responsible for supporting the Program Manager (PM) on all aspects of the test and evaluation effort, including:

[33] DoDI 5000.87, pg. 18

- T&E program strategy, design, development, oversight
- Analysis, assessment, and reporting test results

The PM should charter the T&E WIPT during the Planning Phase so that it is involved with the program's Acquisition Strategy, contract requirements for T&E, and test plan development. The T&E WIPT also assists the PM in managing the T&E program throughout the lifecycle of the software acquisition. The PM should also ensure that T&E resources and other requirements needed to adequately plan and execute the T&E program are coordinated with the T&E community (to include operational test community). T&E resources should be articulated in requests for proposals (RFPs) and other acquisition documents that will affect the contractual requirements and availability of information to the T&E WIPT.

The T&E WIPT consists of representatives from all organizations responsible for providing or overseeing the T&E Strategy and its execution. In particular, the T&E WIPT should include test data stakeholders such as systems engineering, the Lead Developmental Test Organization, Chief Developmental Tester, Operational Test Agency (OTA), D,DTE&A (for programs on DTE&A oversight), DOT&E (for programs on DOT&E oversight), cybersecurity lead, interoperability evaluator, the Capability Owner, and applicable certification authorities. Roles and responsibilities for T&E WIPT members and participants should be documented in a T&E WIPT Charter.

In developing the T&E Strategy, the T&E WIPT should ensure it is executable and aligns with the acquisition strategy, T&E policy (DODI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. T&E Strategy development, content, and approval is described further in Section 2.1.

The T&E WIPT should participate in requirements definition and refinement activities to understand the rationale behind the requirements, and to ensure their measurability, testability, and achievability. These activities should address both high-level needs and evolving requirements. The PM should ensure that the T&E WIPT is enabled to coordinate with the requirements authority to clarify any requirements found untestable.

1.5 Roles and Responsibilities

1.5.1 Developmental Test Teams

In iterative development, increased collaboration among independent test teams and developers and users is required.

- Development teams will lead lower level tests such as unit tests, whereas independent test teams will lead integration and acceptance tests. Results from all testing should be captured in a shared body of evidence, a data repository to store test data that all parties can use for independent evaluation.
- Test teams should be involved up front to ensure they get the data they need from the developmental test process.
- Test teams should strive to maintain a tempo for release testing in sync with the development team(s) by using automation for functional, performance, and regression testing.

- Government test teams should develop a robust T&E at the feature and release level with end-to-end mission threads and employing actual users. Refer to Sections 3.2.2 through 3.2.4.
- Evaluating and adjusting the DT&E strategy within the T&E Strategy to stay current with the Capability Needs Statement (CNS).[34] For programs on oversight, D,DTE&A will monitor and adjust the DT&E strategy and oversight involvement.

Development testing will likely employ automated test tools for functional and cyber testing, which will require the government testers to understand and use these tools.

1.5.2 Operational Test Teams

OT&E concentrates on appropriately scoped, dedicated tests while integrating information from all sources to provide usable data that meet stakeholder needs and inform decision makers. The OT&E effort during this phase includes participating via the test activities of each iteration and through dedicated tests to build a shared body of evidence.

Appropriately scoped OT&E aligns with deployment decisions associated with the MVP and the MVCR. Following the MVCR, OT&E continues to follow a risk-informed approach that scopes tests and evaluations to the capabilities delivered. Software Acquisition Pathway programs will spend the majority of their lifetime in risk-informed OT&E following the MVCR.

A risk-appropriate OA is usually required in support of every limited deployment.[35] The OTA should conduct this risk assessment based on DOT&E and Service guidance. For programs on DOT&E oversight, DOT&E approves the risk assessment and operational test plans.

The OT&E strategy includes:

- Scoping the tests to match the capability delivered and proposed for deployment for operational use, and identifying opportunities for OT&E involvement within all Execution Phase activities. The OTA will consult the PMO and DOT&E, for programs on oversight, to scope the tests. DOT&E approves the operational test plans for programs on oversight.
- Providing operational evaluations to inform decisions and products of the Software Acquisition Pathway, including deployment of software releases and program decisions; an important product to support is the annual Value Assessment.
- Evaluating and adjusting the OT&E strategy within the T&E Strategy to stay current with the Capability Needs Statement (CNS); for programs on oversight, the OTA and DOT&E will monitor and adjust the OT&E strategy and oversight involvement.
- Embedding into the software development and testing process during the Execution Phase to collect data from development needed to scope OT&E and support operational evaluations; embedding includes having continuous visibility into the development process, but does not imply that OT&E should develop the software.

[34] Refer to Table for definition of the CNS.

[35] DoDI 5000.89, p30

Embedding OT&E within the development process requires OT&E participation via electronic and physical presence in the activity of the software pipeline or factory. This includes:

- Monitoring the tests that occur throughout the development pipeline to understand and trust the veracity of the automated and manual testing results to support operational evaluations (the OTA should independently Verify, Validate, and Accredit (VV&A)[36] any automated test capabilities that will provide data supporting operational evaluations)
- Participate in defining test requirements that include end-to-end mission threads
- Ensuring the pedigree of test processes establishes the trust for integrating across different types of testing and remotely monitoring tests
- Monitoring the deployment of new software to the production or live environment to inform the evaluation of capability deployment
- Confirming the presence and functionality of deployment procedures provides for continuity of operations, especially for programs deploying software in short time frames, such as continuous delivery strategies

Additionally, the supply chain for the software includes the pipeline, and how its characteristics affect the software. Testers should conduct cybersecurity testing of the pipeline processes that could lead to exploitation of the software under development, and evaluate how the process for moving software from staging to production will affect deployment and influence cyber defensive operations training. The PM should provide testers with information about the software supply chain and pipeline to support test planning and evaluation.

For each increment, even those not intended for deployment, the OTA should observe testing to determine the applicability of the data for OT&E, including the mapping of that data to the critical assessment areas, and identify gaps in data that will inform test planning for future iterations. The OTA should provide a summary of these items to the PM and, for programs on DOT&E oversight, DOT&E.

1.5.3 Additional Software Pathway Roles and Responsibilities

Iterative software development introduces new roles with the user being represented early and throughout the development process. Figure 3 presents a notional description of how these new user roles relate to the traditional software acquisition roles. This is not intended to be a comprehensive list capturing the responsibilities of all stakeholders in the program community, but rather the key relationships between operations/requirements and acquisition leaders.

[36] Testers should refer to the Modeling and Simulation Focus Area for additional information on VV&A.

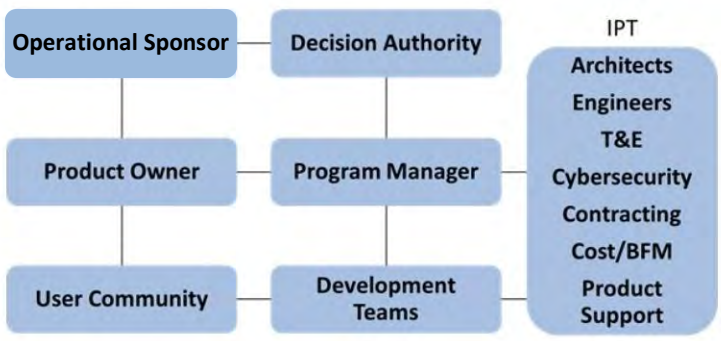


Figure 3. User Roles in Iterative Software Development

Operational Sponsor. The senior leader that champions the operational needs/requirements and funding, the Operational Sponsor represents the DoD organization(s) that will be the eventual users of the software solution, and:

- Defines the desired value that the solution will provide
- Approves the high-level Capability Needs Statement (CNS)
- Approves the User Agreement (UA) with the PM and provides users for the PM
- Identifies the Product Owner and co-chairs value assessments
- Ensures users and stakeholder inputs are captured and integrated into value assessments

Product Owner.[37] Representing the Operational Sponsor at the program level, the Product Owner:

- Develops the CNS to sufficient detail to guide the execution phase and develops UA, in coordination with the PM, to identify user resources to support the execution phase
- Is responsible for day-to-day requirements management
- Coordinates user community representation and participates with them in requirements identification and prioritization. Works with the PM to scope the MVP/MVCR and manages and prioritizes the program backlog
- Approves acceptance at the feature or release level and validates releases and user acceptance tests
- Works with the Product Owner(s) assigned to the program; leads the periodic value assessment of the software solution

User Community. A group of personnel allocated to support the program through the UA that represent the various persona who will employ the system in military operations.

- Provides acquisition and development communities insights into the operational environment.
- Provides meaningful feedback and evaluation of software developed.
- Participates in demonstrations and testing activities.

[37] Note that some Agile Development documents identify a "Product Owner" as part of the development team, which is different from this Product Owner. The Product Owner on the PM's development team is the PM's interface to the user community to ensure the requirements reflect the needs and priorities of the user and align with mission objectives

2. T&E During the Planning Phase

The purpose of the Planning Phase is to better understand users' needs and plan the approach to deliver software capabilities to meet those needs. During this phase, various stakeholders are developing documentation, summarized and defined in Table, and the testing infrastructure, tools, and data. This section explains the role of T&E in this process needed to set the conditions for success during the Execution Phase.

Table 2. Planning Phase Documents

Artifact	Description	Developed by
Test and Evaluation Strategy a	Defines the processes by which capabilities, features, user stories, use cases, etc. will be tested and evaluated to satisfy developmental test and evaluation criteria, and defines the processes by which the system will be tested to demonstrate operational effectiveness, suitability, interoperability, and survivability.	Program Manager with the T&E WIPT
Capability Needs Statement (CNS) a	A high-level capture of mission deficiencies, or enhancements to existing operational capabilities, features, interoperability needs, legacy interfaces, and other attributes, that provides enough information to define various software solutions as they relate to the overall threat environment.	Sponsor with support from the Program Manager
User Agreement (UA) a	A commitment between the Sponsor and Program Manager for continuous user involvement and assigned decision-making authority in the development and delivery of software capability releases.	Sponsor and Program Manager
Acquisition Strategy a	An integrated plan that identifies the overall approach to rapidly and iteratively acquiring, developing, delivering, and sustaining software capabilities to meet users' needs.	Program Manager
Intellectual Property (IP) Strategy a	Identifies and describes the management of delivery and associated license rights for all software and related materials necessary to meet operational, cybersecurity, and supportability requirements. The IP strategy should support and be consistent with all other government strategies for design, development, test and evaluation, operation, modernization, and long-term supportability of the software, protection of the software supply chain, and should be implemented via appropriate requirements in the contracts.	Program Manager
Cost Estimate	Developed in accordance with DoDI 5000.73 (Cost Analysis Guidance and Procedures). The estimate should consider the	Program Manager

Artifact	Description	Developed by
	technical content of the program described in the CNS, UA, acquisition strategy, and test strategy.	
Request for Proposals	A document used in negotiated acquisitions to communicate government requirements to prospective contractors and to solicit proposals.	Program Manager

a DoDI 5000.87, "Operation of the Software Acquisition Pathway"
b DAU Glossary

2.1 T&E Strategy

The purpose of the T&E Strategy is to guide the activities of test organizations in planning and executing an effective and efficient test process in support of the program and major program decision. The T&E Strategy is the high-level test planning document for the Software Acquisition Pathway.

The T&E Strategy serves as a contract between the PM and all T&E stakeholders for T&E roles and responsibilities, and resources. The T&E Strategy captures processes by which capabilities, features, user stories, use cases, etc., will be tested and evaluated to verify technical requirements; it should also capture the process by which the operational effectiveness, suitability, and survivability of the system will be evaluated. This testing process should be integrated between the contractor testing, developmental testing, and operational testing teams to provide a holistic view of the system. The T&E Strategy should capture the missions the system is intended to perform, evaluation of the system in the context of a unit equipped with it, and all interfacing systems.

The T&E Strategy should identify evaluation focus areas and critical assessment areas from which test teams derive their data requirements to support major program decisions. However, additional critical assessment areas may be included in system evaluation. Further, the T&E Strategy describes the test events and activities that will provide the data necessary to evaluate the system and support acquisition, technical, and program decisions – termed an Integrated Decision Support Key (IDSK) in DoDI 5000.89, which outlines the integrated approach to testing. The T&E Strategy should describe how these data will be accumulated to build a shared body of evidence to support evaluations of the system. Refer to Section 0 for more information about establishing and maintaining the shared body of evidence. Descriptions of cyber testing in the T&E Strategy should align with content described in the Cyber T&E Focus Area.

The Decision Authority approves the T&E Strategy prior to the program entering the Execution Phase. For programs on DOT&E oversight, DOT&E is the final approver for the T&E Strategy.[38] The T&E Strategy should be updated as needed to align with the current Capability Needs Statement.

[38] DoDI 5000.87, p 14

2.1.1 Data

The T&E Strategy should identify the data required to adequately evaluate the system's technical, functional, and operational performance to inform acquisition, technical, and program decisions, and outline an integrated approach to properly size test events and share data. In addition, it should define the conditions under which these data will be collected, and any tools required to manage the data and perform the testing.

2.1.2 T&E Resources

The T&E Strategy should determine the T&E resources required to support it (e.g., facilities, ranges, operational force structure, cyber ranges and test teams, instrumentation and associated support, automated testing tools, software systems integration labs, modeling and simulation (M&S), including the organization that will validate the models, and costs). The strategy should also identify shortfalls that will require investments to meet T&E infrastructure sufficiency, and plan for any Verification, Validation, and Accreditation (VV&A) activities required to accredit the T&E infrastructure for operational test events. T&E funding in the resources section should be consistent with the cost estimate and budget submissions.

2.2 T&E Content and Interests in Other Planning Phase Documents

While the T&E Strategy is the main testing deliverable during the Planning Phase, it relies heavily on each of the other documents outlined in Table. The T&E community should work with the acquisition community on these documents to incorporate needed T&E information. This section highlights T&E content and involvement of test teams in the development of each of these documents.

2.2.1 Capability Needs Statement (CNS)

Test teams should be involved with CNS development early to fully understand the desired capabilities and ensure that these requirements focus on the mission capability. The test teams should also work with their engineering counterparts to ensure requirements traceability from the capability level requirements to user stories exists so that the test teams can evaluate the system.

Test teams should:

- Define the level of requirements best suited for government T&E
- Understand what constitutes "value" and how that will be measured at value assessments after deployments (annually)
- Ensure cyber and interoperability needs are clearly defined in the CNS

While the Software Acquisition Pathway does not require the Joint Capabilities Integration and Development System (JCIDS) process, test teams can use the JCS Cyber Survivability Endorsement and Implementation Guide[39] to define cyber attributes within the CNS.

[39] JCS Cyber Survivability Endorsement and Implementation Guide

2.2.2 User Agreement (UA)

The Software Acquisition Pathway emphasizes user involvement in development. The DoDI 5000.87 requires that software development be done in active collaboration with end users, representing key user groups, to ensure software deliveries address their priority needs, and undergo regular assessment of software performance and risk. The goal of this continuous user engagement and feedback process is to develop software that best satisfies users' needs.

During the UA development, test teams should:

- Ensure the UA includes user participation in government testing to serve as test operators and provide feedback, including support from users and units for test and evaluation as needed
- Establish early contact with the user community and understand how the users expect the system to work

2.2.3 Acquisition Strategy

The Acquisition Strategy should sufficiently describe the development and decisions to convey what information/data testing needs to provide, and when, as well as account for test and evaluation when identifying resource needs.

The Acquisition Strategy sets the schedule within an initial product roadmap (Section 3.1) for delivering the initial capability and the subsequent cadence for delivering additional capabilities. Test teams should:

- Ensure that test requirements and data delivery for the contractor are thoroughly outlined and included with more detail in the RFP
- Ensure that time is allotted in the program schedule for independent government T&E
- Ensure that the Acquisition Strategy addresses a robust cyber T&E program, including the supply chain
- Understand the decision points that will require test data to make informed decisions (for embedded software, this includes the decision points for the system on which the software is embedded)

In addition, the Acquisition Strategy requires a high-level T&E Strategy that describes plans for verification and validation of software quality, integration and automation of testing, and citing the required test platforms, resources, and infrastructure. Test teams should:

- Ensure the test and evaluation strategy portion of the Acquisition Strategy provides a clear description of the test approach, including any M&S needs, so that it can be included in program planning and the separate T&E Strategy document. For embedded systems, this should align with the testing strategy for the system on which the software is embedded.

2.2.4 Cost Estimate

The cost estimate should consider the technical content of the program described in the CNS, UA, Acquisition Strategy, and T&E Strategy. Test teams should ensure that the cost estimate includes all the resources necessary to conduct testing.

2.2.5 Intellectual Property (IP) Strategy

Test teams should provide input to the IP strategy on the ownership of data generated (such as contractor-generated test results) during all phases of testing that would allow building a shared body of test evidence, available to the program throughout its lifecycle. The PM should further consult with the T&E community to determine any access needed to support independent testing and include these accesses in the IP strategy as needed.

2.2.6 Request for Proposal (RFP)

The RFP defines what the government expects from the contractor; if it is not in the RFP and the eventual contract, you will not get it. The T&E Strategy is a source document for the RFP.[40] The PM should consult with test teams to ensure that the RFP supports data collection for government T&E.

At a minimum, a draft T&E Strategy should be included as an attachment to the RFP to clearly tell the contractors what the government-intended testing is.

The test teams should ensure that the following items and activities are requested:

- Government access to contractor test events, M&S, test tools, test data repositories, and test environments
- Contractor test plans, procedures, reports, and data
- Contractor support for government testing

2.3 Test Infrastructure, Tools, and Data

In addition to the documentation, the Test Infrastructure is also established during the Planning Phase, during which test teams should work with the PM as they develop the infrastructure to identify how test data from different environments can be used to support evaluations. For example, data used to support operational test and evaluation should be generated within an operationally representative environment. If the environment is not operationally representative, limitations to the environment should be enumerated and operational evaluations should be based on the context of the environment in which the data were generated. Section 2.3.1 describes different environments and evaluation of these environments for different testing uses.

Likewise, these environments may need to be instrumented with different testing tools to gather metrics needed to support evaluations. Section 2.3.2 describes this instrumentation and evaluation of tools for different testing uses.

Lastly, in order to establish an integrated evaluation approach, data should be shared among all parties. Section 0 describes this sharing of data.

2.3.1 Test Infrastructure

2.3.1.1 Pipelines and Software Factories

To provide for continuous integration and delivery of software to the customer, modern software development has adopted infrastructure frameworks. These frameworks allow for consistent and

[40] DoDI 5000.89, p14

repeatable processes to be followed, and provide visibility into those processes, enabling a level of trust to all functional personnel throughout the lifecycle. Developers, test teams, security engineers, product owners, and users have a common foundation on which to build their processes. It is this core orchestration framework, commonly called a "pipeline," that provides this foundation.

- A pipeline is a collection of tools, processes, and environments designed to move code from the development environment to the production environment. These environments connect much like a physical assembly line, with the output of one environment becoming the input of the next.
- A software factory contains multiple pipelines equipped with tools, process workflows, scripts, and environments to produce a set of software deployable artifacts with minimal human intervention. It automates the activities in the develop, build, test, release, and deliver phases of the Development, Security, and Operations (DevSecOps) lifecycle.

Pipelines and software factories have a cadence for developing and delivering software. Testing, including operationally representative test cases, should be included in this cadence to support the software development.

2.3.1.2 Test Environments

Within the pipelines, there may be a number of environments where testing may take place:

- **Sandbox:** A sandbox, not necessarily in the pipeline for DevSecOps, is an isolated environment to prevent any possible damage to other environments. It is used for early adversarial cyber-testing and may be used for experimentation.
- **Development (Dev):** The Dev environment is for the development of code and is the environment where iterative development teams normally operate. Test teams, as part of the development team, use the Dev environment to test software units.
- **Integration:** The integration environment is where the software units from multiple development teams come together for testing at a higher level (e.g., features or capabilities). While the software developer may own the integration environment, it is a good place for government test teams to observe and collect some test data that may reduce the need for repeated testing later.
- **Test:** Sometimes called “quality assurance (QA),” the test environment is where developmental and integrated testing is conducted at the system or system-of-systems level. It is normally the last opportunity for developmental testing (except for possible User Acceptance Testing) prior to release to the operations team. The software that comes out of the test environment bears the mark of quality from the development and testing starting at the development team level.
    - The Test Environment should represent the production environment as closely as possible, including monitoring capabilities and the ability to simulate realistic system usage. It might not, however, connect to production environments of interfacing systems within the system of systems.
    - The Test Environment may instead connect to test environments of interfacing systems. Program offices should plan early to coordinate access to interfacing system test environments. These interfacing systems provide the basis for initial interoperability testing. When testing within these environments, it is important to not only test the transmission and receipt of messages, but also the effect of these

messages on the interfacing system. If interfacing test environments are not available, it is incumbent on the program to obtain or develop models or simulations of the interfacing systems and incorporate them into their test environment.
    - Enterprise, artificial intelligence, and machine learning capabilities all rely on ingesting data from multiple data sources, and data integration efforts should run parallel with the software development to make sure the data is in useful form when the software is ready. The data integration should begin in the development of each iteration, but needs to be demonstrated in comprehensive DT before OT.
    - M&S may be employed to represent a production environment that is difficult to replicate or does not currently exist, such as hardware platforms with long build times, data feeds, and interfacing systems. Some systems (such as weapons systems) will need extensive M&S to properly simulate mission conditions.

- **Pre-production (Pre-Prod):** Sometimes called "staging" or "soaking," this is the environment for user acceptance testing, a testing event that verifies the operation of the software in a production-representative environment, including representative cyber threats, prior to full release.
- **Production (Prod):** The production environment, used for live operations with real operators, is often the environment for formal operational testing, and supports the acceptance of the software by the government and the "go live" decision to shift the new software to live operations.

T&E success during the Execution Phase depends on the PM, working with the T&E WIPT, identifying the environments necessary to execute testing for the evaluation focus areas during the Planning Phase and establishing them to the extent feasible. The ability of T&E to remain involved and responsive to the anticipated cadence of software development using continuous integration and delivery starts with testing in operationally representative environments. This is applicable for both the applications and embedded paths.

The environments used to conduct testing for OT&E should represent the production environment as closely as possible, including monitoring capabilities and realistic system use. This requires a high-fidelity representation of the interfacing systems that form the system of systems with the program of record.

The OTA should VV&A the pre-production environments and tools planned for OT&E use before the program enters execution to support the software development cadence. This VV&A should consider data collection, interfacing systems and databases, networks, simulated environments, simulated users, and ranges.

2.3.2 Test Tools

2.3.2.1 Test Automation

Software testing, both functional and cyber testing, should be automated as much as possible to support continuous integration and delivery. The scale of software and the associated testing is

too large for only manual testing, and activities such as regression testing[41] and testing of the routine and repeated human interfaces can benefit greatly from automation. Continuous development, integration, and delivery of software cannot be accomplished without automated T&E.

Automated test tools fall into two major categories:

- **Test management tools** automate the process of test planning, scheduling, tracking, and reporting test events.
- **Test execution tools** automate the process of executing test cases or procedures on the system under test.

The Test Lead should work with the contractor to fully understand the contractor's tools and ensure tools that support OT&E are independently VV&A'd for use. Government test teams should be trained with these tools so they can use their outputs across the software development process to inform evaluations.

Frequently, there will be automated tools supporting multiple phases in the development pipeline, and interoperability among these tools can become a problem. Using known frameworks for pipelines and software factories, as discussed earlier, can help overcome these issues, as it should be inherent in the infrastructure, though testers will still need to identify the data mapping from the automated tools to the evaluation areas.

Automated testing is for government as well as contractor test teams, and using the same tools as the contractor is advantageous for the government (e.g., easier to replicate events when necessary). In some cases, government test teams should become experts in the tools used by both the contractor and other government teams. The automated tools should also provide visibility into the continuous testing occurring within the pipelines so that stakeholders can gain confidence on the quality of the development process.

2.3.2.2 Tools for Data Collection and Reduction

The test teams should first identify the measures to evaluate the system, as well as the data needed and conditions under which it will be collected. These conditions should include injecting operationally representative input values and providing simulated environments to emulate the outcome of the given injects. Additionally, capturing of user interaction with the system should be automated to the extent practical. Having identified the data needs, they should then identify the tools necessary to produce the identified test conditions and collect, reduce, and analyze the data. This should include an evaluation of currently available options and existing system software eco-systems and infrastructure. The needed tools should be integrated into the software pipeline to provide the necessary data. A tabletop exercise can assist in confirming the feasibility of the proposed plans, tools, and methodology.

The test teams should work with the PM as applicable to ensure these tools are available and resourced. The use of these tools should be included in the T&E Strategy.

[41] Regression testing is re-running functional and non-functional tests to ensure that previously developed and tested software still performs after a change.

2.3.3 Test Data: Shared Body of Evidence and Data Repository

During the Planning Phase, the PM should establish a secure data repository to store test data and provide access to all test teams so that they can review, use, and input these test data. Throughout the software development, T&E should be building a shared body of test evidence to support technical, functional, and operational performance evaluations. Relevant test data gathered through all testing should be included in this test data repository. The OTA should maintain the authoritative data for OT&E.

3. T&E During the Execution Phase

Following the Planning Phase, the program will enter the Execution Phase, the purpose of which is to rapidly and iteratively design, develop, integrate, test, deliver, operate, and monitor resilient and reliable software capabilities that meet users' priority needs.[42] The Execution Phase comprises a series of iterations of "plan, code, build, test" to develop software that meets users' needs. As a cyclic and iterative development, it is important to have both DT&E and OT&E test teams involved in testing throughout the Execution Phase to support their independent evaluations.

The Software Acquisition Pathway delivers software in small increments at a prescribed cadence, and T&E should be integrated with that cadence. The result is testing that is continuous throughout the product's lifecycle, with several types of test conducted during the delivery cadence. At times, the program may hold increments from deployment to be combined with others and deployed as a larger release, which may require discrete testing. Test teams should plan for both continual and discrete testing.

Testing should be scheduled based on the product roadmap. Details of this roadmap and its use for T&E are detailed in Section 3.1.

The testing during the Execution Phase can be divided into two areas: testing throughout the development and testing of individual releases. These both support independent government evaluations. Sections 3.2 and 3.3 describe the two areas of testing, respectively. Section 3.4 further describes how data collected from monitoring fielded software can support evaluations.

Lastly, the annual value assessments should be informed by test and evaluation results. Section 3.5 describes how T&E may work with the Program Office to collect data that supports these assessments. The value assessment does not replace operational testing, and the of which is addressed in Section 3.3.

3.1 Product Roadmap

The product roadmap is derived from the Capability Needs Statement and breaks down the required capabilities into epics and features[43]. The product roadmap is "a high-level visual summary that maps out the vision and direction of product offerings over time. It describes the

[42] DoDI 5000.87, p16

[43] An epic is a large body of work to be completed during development. Epics are further decomposed into smaller features and user stories. Refer to the Agile 101 document for additional information: https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/Agile%20101%20v1.0.pdf

goals and features of each software iteration and increment."[44] An iteration typically refers to a unit of time, whereas an increment refers to a unit of software.

"Programs use the product roadmap to communicate when capability is projected to be delivered. A product roadmap provides a rolling calendar-based view of key capabilities/feature sets to be delivered in the near term (10–12 weeks) through the coming 12–18 months for a product/service, and a high-level description of capabilities to be delivered annually. The roadmap is considered a product schedule."[45]

As a product schedule, the roadmap assists the testers in identifying what epics and features will be developed and tested over time, and thereby influences the detailed test planning and schedule. Figure 4 is a notional roadmap showing how epic and feature development results in capability delivery over time. Though not shown in this notional figure, product roadmaps should define a time period for each iteration. Note that, as with other iterative development plans, it is flexible and subject to change to meet users' emerging requirements and priorities. Test teams should be aware of this flexibility and be prepared to respond as needed. For operational testing, this may include revising risk assessments based on capabilities planned for delivery compared to the capabilities needed. PMs should communicate changes to test teams as they are made to enable adequate response.

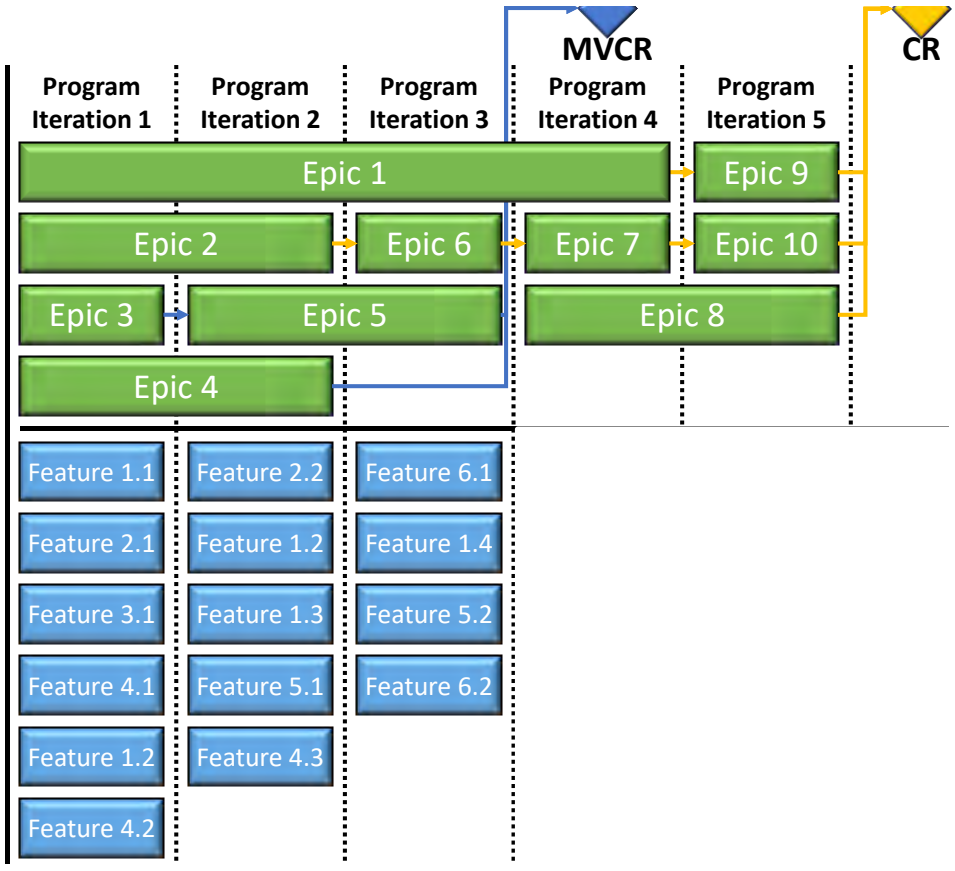


Figure 4. Notional Roadmap[46]

[44] DoDI 5000.87, Glossary

[45] DAU AAF Software Pathway Define Capability Needs

Other things to note from Figure 4 are:

- Capability Releases (CRs)[47], including the Minimum Viable Capability Release (MVCR), are prime candidates for independent government T&E (including OT&E). Refer to Section 3.3 for additional information about scoping capability release testing.
- Not every program increment needs to be deployed to the users.
- Completed epics may not coincide with the next capability release (e.g., Epics 2 and 6 in Figure 4 going to the next CR after the MVCR).

3.2 T&E throughout Iterative Software Development

Government test teams should participate in the iterative development process to review and accept testing conducted iteratively as sufficient, in order to reduce the scope of future government testing. To facilitate this, program offices should ensure government test teams have visibility into contractor testing activities and, results, and complete access to the issue tracking system.

The goal of observing and participating in the planning and demonstration is to capture test data to build a shared body of evidence that can be used as part of the government evaluation to verify whether detailed requirements at the story and feature level are satisfied. Educating the developer on test practices/techniques can be a good practice for improving quality. The intent is to incorporate test cases and scenarios of interest to the government early in the development process and thereby avoid having to re-test these requirements as a subsequent government test. Manual penetration testing and interactive application security testing at the end of each sprint may include misuse and abuse testing to ensure system resilience and cyber survivability.

The T&E community should develop and tailor evaluation metrics for each capability release, then build a data collection, analysis, and reduction plan. While each development iteration may not lead to a capability release, data from each development iteration should support evaluation of the capability release. Ideally, the plan for the capability release will use already existing testing plans and frameworks, tailored to current needs. The T&E community should provide an assessment or evaluation to decision authorities to contribute to decisions and the shared body of evidence.

Within and across capability releases, epics and their features should trace to the identified user capability needs. The T&E community should understand and confirm the traceability among the epics, features, and user capability needs. The T&E community will collect information on how they fit within the larger system of systems for the program. Finally, the T&E community should observe the testing and approval of the features to understand the context of the test environment.

---

[46] Adapted from DAU Course ACQ 1700: Agile for DoD Acquisition Team Members

[47] This document uses the term Capability Release to refer to software to be delivered to users for operational use.

The T&E community will need to understand and participate in the process for developing user stories[48] from the features and validating that the user stories reflect user expectations. Confirming the process for user story traceability to capability needs and decomposition into software tasks informs the evaluation and understanding of test results. The T&E community should review processes, understand the traceability, and assist where needed. A key consideration when reviewing the user stories is to ensure inclusion of all relevant user personas present in the deployed operational environment.

In iterative software development during the Execution Phase, testing is a part of the continuous process that requires integration between testing and development and users to achieve high product quality. Test teams should be involved up front to ensure they get the data they need from the process.

A primary example of early test involvement is Test Driven Development (TDD), in which Dev Team testers develop test scripts, derived from the user stories, that provide details of what the software should do to be declared "done." Dev Teams then develop software to pass the test scripts. Some programs have experimented by placing government testers in these roles to better understand the software development process and participate in early verification. In these cases, TDD places a lot of responsibility on government testers to work closely with the capability owner, learn how to write and execute test scripts, and define and declare the "definition of done." If resources are limited, government testers may not be able to be embedded in the Dev Teams, but they should still understand how to write and read automated test scripts to monitor and collect test data from vendor or government Dev Team testing.

Two variations of TDD include Behavior Driven Development (BDD) and Acceptance Test Driven Development (ATDD). This is where government testers should have significant involvement. BDD looks at a class of user stories (e.g., a scenario) and tests to "the specifications of the behavior of the class" that produces an outcome valuable to a user.[49] Rather than using the "as a role-I-want-so-that" format of a user story, BDD uses a "given-when-then" format.

GIVEN: The preconditions of the test (e.g., my system is connected to all necessary external sources).

WHEN: An action is taken (e.g., I request a status of friendly forces).

THEN: The following results should occur (e.g., the location and status of friendly forces are displayed).

Note, it is also possible to add "**AND**" statements to better define the behavior (e.g., AND I specify the information I need).

ATDD derives from both TDD and BDD, but at a higher level, looking at the overall customer experience. According to a Net Solutions blog, TDD asks "are we building the thing right," BDD asks "if the thing is behaving as expected," and ATDD asks "are we building the right thing."[50]

---

[48] A user story is the smallest unit of requirements written from a user's perspective of how they will use the software. Refer to the Agile 101 document for additional information: https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/Agile%20101%20v1.0.pdf

[49] agilealliance.org/glossary/bdd

[50] Net Solutions blog

ATDD often uses the same given-when-then format of BDD, but at a higher level. Table 3 provides a comparison of TDD, BDD, and ATDD. As noted above, government testers should focus on BDD and ATDD.

Table 3. Comparison of TDD, BDD, and ATDD[51]

Parameters	TDD	BDD	ATDD
Definition	A development technique focused on individual units of a desired feature	A development technique focused on expected behavior	A development technique focused on meeting the needs of the user
Participants	Developer	Developers, Customer, testers	Developers, Customers, testers
Language Used	Written in programming language used for feature development (e.g., Java, Python, etc.)	Gherkin / Simple English	Gherkin / Simple English
Understanding Tests	Tests written by and for developers	Tests written for anyone to understand	Tests written for anyone to understand
Focus	Unit Tests	Understanding Requirements	Writing Acceptance Tests
Bugs	Reduced likelihood, easier to track down	Can be more difficult to track compared to TDD	Can be more difficult to track compared to TDD
Suitable For	Projects that do not involve end users (server, API, etc.)	Projects which are driven by user actions.	Projects where customer experiences are important and competition is high
Tools Used	JDave, Cucumber, JBehave, Spec Flow, BeanSpec, Gherkin Concordian, FitNesse, Junit, TestNG, NUnit frameworks, Selenium tool (any open source tools)	Gherkin, Dave, Cucumber, RSpec, Behat, Lettuce, JBehave, Specflow, BeanSpec, Concordian, MSpec, Cucumber with Selenium / Serenity	TestNG, FitNesse, EasyB, Spectacular, Concordian, Thucydides, Robot Framework, FIT

[51] Ibid.

Figure 5 and Table 4 summarize the different testing types during software development that may occur during the Execution Phase. These are each detailed further in Sections 3.2.1 through 3.2.6.

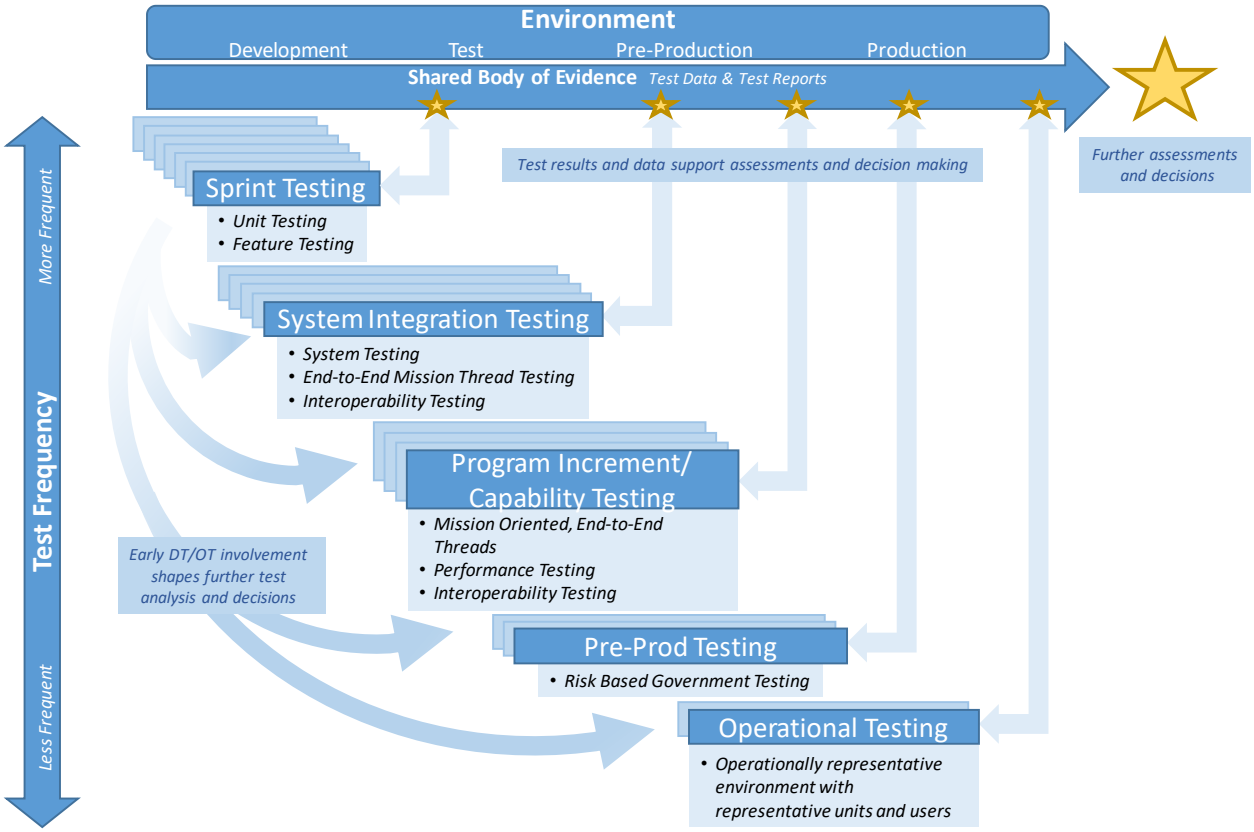


Figure 5. Continuum of Test Throughout the Development Lifecycle

Table 4. Summary of Testing Types During Iterative Development

Testing Type	Summary of T&E Guidance	
Agile/Sprint	• Developer runs unit tests and conducts demonstrations at the end of each sprint. OT Team can conduct user surveys during demonstrations to support early suitability assessments.	Cybersecurity Testing [a]
System Integration	• End-to-end mission thread testing (including cyber and interoperability testing). • Requires a secure test environment that closely resembles the production environment, a comprehensive build of the software, data that exercises the connections inside and outside the application, and a test plan.	
Program Increment or Capability Release	• Government-led DT event to verify that the system capability is ready for release to the operational user. • DT team should coordinate this testing with OT and interoperability (e.g., JITC) test teams to facilitate early collection of test data for independent OT&E and certification.	
Pre-production	• Operations team conducts testing to resolve any potential problems because of differences between the development environment(s) and production environment(s). • Lead DT&E Organization or OTA can conduct risk-based government DT or OT on the pre-production environment, and government cyber testers test with less risk of affecting actual operations.	
Operational (e.g., Operational Assessment, Initial Operational Test, Limited User Test)	• OTA conducts testing to evaluate the operational effectiveness, suitability, and survivability (including cyber) of the system, or progress toward, in an operationally representative environment with representative system users and units equipped with the system • OT&E should utilize data from contractor and developmental testing for system functions and focus on the software's ability to support end-to-end mission(s).	

[a] Cybersecurity testing should evaluate the system throughout development and all test phases to determine cyber posture and include in independent, government events to support evaluation

3.2.1 Agile /Sprint Testing

The developer runs unit tests upon implementing a user story, using pre-written test scripts to verify success or failure. The test scripts automate the testing and provide a repeatable process to verify software performance. Ideally, user stories combine into features that provide the user a better perspective of the operational value of the software. Just as the user stories are integrated to form features, the test scripts are integrated to automatically test software at this higher level.

This automated union of user story testing does not necessarily imply that the feature testing is complete. Early cyber testing at this level should include at a minimum static and dynamic analysis to identify known vulnerabilities.

The development team conducts demonstrations at the end of each sprint to show users how all the software units work together and to provide hands-on experience and gain user feedback. Actual user participation is important to get feedback, early acceptance, and buy in. The OT team can conduct user surveys during these demonstrations to support early suitability assessments.

3.2.2 System Integration Testing

Integration testing brings together the individual efforts and outputs of multiple development teams to test at the system level with end-to-end mission thread testing (including cyber and interoperability testing). This testing requires a secure test environment that closely resembles the target (or production) environment, a comprehensive build of the software, data that exercises the connections inside and outside the application, and a test plan (including test cases developed by the contractor and the government). The system integration testing should also include testing representative interfaces with external systems using representative data.

3.2.3 Program Increment or Capability Release Testing

The release test is a government-led DT event to verify that the system capability is ready for release to the operational user. Coordinating this testing with OT and interoperability test teams (as applicable) is encouraged to facilitate early collection of test data for their independent evaluation or certification. Capability Release testing is a key activity to support the decision authority in making informed release decisions. The Capability Release test should focus on mission-oriented DT with end-to-end mission threads and actual users. Testing should also include cyber DT, performance/load testing, and interoperability testing.

3.2.4 Pre-production Testing

The operations team[52] conducts testing to resolve any problems that might be caused by a difference in configurations between the development or test environment and the pre-production or production environment. Ideally, there should be no differences, but this may not always be the case. Testing on the pre-production environment is also where the Lead DT&E Organization or OTA can conduct risk-based government DT/OT and the government cyber tester can conduct testing with less risk of impacting actual operations.

3.2.5 Operational Testing

Operational testing and evaluation should be conducted to support MVP, MVCR, and subsequent capability releases.

These operational evaluations should utilize data from contractor and developmental testing for system functions (where feasible) and focus on the ability for the software to support the end-to-end mission of the users. Data for operational evaluations should include use by operators and

[52] The operations team includes system administrators, database managers, network managers, and cyber defenders.

units equipped with the system who were not involved in the development testing and software definition to evaluate whether the system will meet the needs of all users.

Software releases that are initial or greatly change capability require user- and unit-level training to develop tactics, techniques, and procedures for use. Often such training periods will include a culminating exercise or activity to ensure that the capability release is ready for operational use. Such activities present an opportunity for collecting data for OT&E.

If the culminating activity is conducted in a pre-production environment, that environment should be validated for operational representativeness and the OTA should note any limitations of the environment. This may include environments already developed for other testing within the DoD. For example, within the embedded path, these may be test environments, including digital representation of hardware, for the platform on which software will reside.

For programs on DOT&E oversight, DOT&E will approve the operational test plan(s) that describes how the OTA will execute operational testing, and which data will be used from the accumulated shared body of evidence to support the evaluation. An operational test plan should be written early in the execution phase, and referenced and updated as needed to support ongoing testing.

3.2.6 Cyber T&E

Cybersecurity testing should be conducted throughout all development and test phases to evaluate the system, including the software pipelines, and determine its cyber posture. Government testing should include both cooperative and adversarial testing.

The test teams should work with the Cyber Working Group, as a subset of the T&E WIPT, early to ensure a coordinated risk management framework and cyber test and evaluation process. Cyber T&E and software assurance will be integral to strategies, designs, development environments, processes, supply chains, architectures, enterprise services, tests, and operations.

The Cyber Working Group is responsible for designing and implementing automated cyber testing and continuous monitoring of operational software to support a continuous authority to operate (cATO) or an accelerated accreditation process to the maximum extent practicable. Results from Cyber T&E will support the cATO throughout the lifecycle.

Automated cyber testing should be augmented with additional testing where appropriate. Programs will also implement recurring cyber assessments of the development and test environments, processes, and tools.

Secured pipelines may improve software security, but additional steps are still required to verify the system itself is resilient to cyberattack. Software assurance and cyber testing activities within and beyond the software factory serve to evaluate that resilience. In addition, periodic assessment of the software factory components is necessary to assure their continued ability to provide a secure environment for software development.

To ensure secure code through the pipeline in the final application, cyber test teams should assess all aspects of the software pipeline. This includes the trusted development platform, tools, processes, and infrastructure. Cyber test teams should assess whether the operator of the development platform maintains trustworthiness through periodic assessments, implementing a

cyber threat intelligence program, regularly installing the latest security updates, and the use of an active defense capability that includes continuous monitoring and logging.

Continuous and automated cyber testing can identify vulnerabilities to help ensure software resilience in the evolving threat environment throughout each sprint and the entire lifecycle. Ensuring software security includes:

- Secure development (e.g., development environment, vetted personnel, coding, test, identity and access management, and supply chain risk management)
- Cyber and software assurance capabilities (e.g., software updates and patching, encryption, runtime monitoring, and logging)
- Secure lifecycle management (e.g., vulnerability management, rigorous and persistent cyber testing, and configuration control)

Testers should evaluate whether the software pipeline provides capabilities to enable iterative development to reduce the burden of full software stack testing and security. Test teams should evaluate, through automated and manual assessment methods, whether all platform, infrastructure, and application security requirements implemented by the development team or inherited by supporting services provide cyber resilience.

Cyber testing should also characterize the cybersecurity defensive status of a system. This includes evaluating the system with the cyber defense team in place.

Program offices adopting iterative development processes to develop and deliver code should incorporate the additional software assurance activities in the Cyber T&E Focus Area and Cyber T&E Companion Guide. The Cyber T&E Focus Area describes cooperative and adversarial cybersecurity testing throughout the lifecycle. The guidebook also offers insight and instruction for performing test activities to evaluate the security of the acquisition program.

3.3 Scoping T&E for MVP, MVCR, and Follow-on Capability Releases

While T&E is conducted throughout development, individual releases should be tested and evaluated as a whole to ensure they are meeting user needs, and are operationally effective, suitable, and survivable. The scope of independent government testing for each release should be determined using a risk-informed strategy.

3.3.1 T&E of the MVP

Government testers should assist the PM with test planning, execution, and data collection and with obtaining feedback from the users. Data collected during an MVP evaluation might be used later for an MVCR evaluation to determine readiness for operational deployment.

The MVP version of the software could become the MVCR if the sponsor determines it is sufficient to be fielded for operational use. In that case, the scope of T&E should increase so as to determine operational effectiveness, suitability, survivability (including cyber), and the risk of mission failure or personal injury in the event the MVP is defective in any manner. Refer to Section 3.3.2.

The scope of the MVP testing is guided by the specific capabilities available and the feedback that the PM and sponsor want to address. This may be limited to user surveys or it might include technical performance testing to help change the design. Since the MVP is essentially a

developmental evaluation, the PM or government developmental testers are prime candidates to lead any MVP testing. To maximize opportunities for integrated testing of the MVP, the PM or government developmental testers should coordinate with the OT&E community for this testing.

As the first version of the software exposed to users, the MVP presents the opportunity for early operational evaluation to assess progress toward operational effectiveness, suitability, and survivability. The OTA should evaluate the MVP in the context of the operational mission(s) the software will support and assess progress toward operational effectiveness, suitability, and survivability. The OTA should incorporate data from the shared body of evidence to support the evaluation.

If the data to support the evaluation will be generated in a virtual environment, the environment should go through VV&A as appropriate to support conclusions. OTAs should indicate any limitations for testing in a virtual environment in the assessment plan.

3.3.1.1 Cyber T&E for MVP

The scope of the cyber T&E of the MVP should be determined based on the maturity of the MVP and the representativeness of its attack surfaces' environment.

If the MVP is mature enough and the assessment is conducted in a quasi-production environment with attack surfaces similar to the production environment, then cybersecurity developmental test events, such as cooperative cyber assessments or adversarial cyber assessments, may be conducted.

Operational cybersecurity testing should also be conducted, as appropriate. At a minimum, the OTA should be gathering metrics and data from cybersecurity testing conducted within the development pipeline.

3.3.2 T&E of the MVCR

As the first capability fielded to support operational missions, the OTA should conduct an Initial OT&E for the MVCR to evaluate its operational effectiveness, suitability, and survivability (including cyber). The OTA should draw data from the shared body of evidence to support the evaluation and the scope the IOT&E. Data gathered during the IOT&E adds to the shared body of evidence supporting the system. DOT&E will independently report on testing of the MVCR for systems on DOT&E oversight.

3.3.2.1 Cyber T&E for MVCR

OT&E of the MVCR should include cooperative and adversarial cyber operational testing. Further details on conducting this testing is included in the Cyber T&E Focus Area and Cyber T&E Companion Guide. The cyber testing of the MVCR may include testing of the software pipeline itself, especially if the pre-production environments of the pipeline are directly connected to the fielded, production environment. This is part of the supply chain assessment.

For programs using the Embedded Pathway, testing the MVCR should be aligned with the IOT&E or other applicable OT&E for the platform on which the software resides.

3.3.3 Risk Informed OT&E for Follow-on Capability Releases after MVCR

OT&E of capability releases should be tailored using a risk-informed strategy. The MVCR testing provides a baseline for testing of future capability releases. Subsequent releases may require less dedicated OT&E based on the risk to mission of the new release being fielded (e.g., complexity of the release, amount of new capability and features included, number of new users involved). The OTA should determine the inclusion of previously tested capabilities in testing based on interactions with new capabilities added and the risk to the mission should they fail as part of the risk assessment.

Programs entering the Software Acquisition Pathway with a capability comparable to an MVCR should follow the risk-informed approach described for capability releases. If operational testing has not yet been conducted, a dedicated OT&E event may be needed to baseline the capabilities and support risk assessments for scoping of future testing.

OTAs should follow the latest DOT&E and Service guidance on conducting risk assessments to determine the level of operational testing. For programs on DOT&E oversight, DOT&E approves the operational test plan.

3.4 T&E Post-Release (Monitoring and Feedback)

To continually evaluate the system, the PMs should provide testers with data from monitoring and feedback of the production system once fielded. Examples of data sources that testers should be provided are:

- System uptime, downtime, and time to repair fixes (e.g., system logs)
- Error reports for specific node hardware, services, and applications
- Help Desk problem reports and their associated closure information
- Cybersecurity monitoring information

Testers should use these data to support ongoing, independent assessments. Monitoring data should be incorporated into the shared body of evidence, as applicable.

Operational testers should use these monitoring data to support independent evaluations of the systems. Use of monitoring data to support operational evaluations should be described in the T&E Strategy, as described in Section 2.1.1. Periodic assessment by operational test teams of the fielded baseline provides objective determination of capability improvement and continued security.

In addition to providing information on the suitability and supportability of the system, the user feedback should inform scoping of future independent testing.

3.5 T&E to Support Value Assessments

The sponsor and user community perform the value assessment annually, which assesses mission improvements and efficiencies realized from the delivered software capabilities, and determines whether the outcomes have been worth the investment.[53] The Value Assessment does not require

[53] DODI 5000.87, p23

separate T&E events, but may use data from T&E to support the assessment. How testing supports the value assessment should be included in the overall T&E Strategy.

The primary concern from the test perspective is: How does the program define "value," and how is it measured? The value assessment satisfies the requirement for a Post-Implementation review (PIR) for an IT system described in DoDI 5000.82, which states that the PIR will "report the degree to which doctrine, organization, training, materiel, leadership, education, personnel, facilities, and policy changes have achieved the established measures of effectiveness for the desired capability.[54]"

The Functional Sponsor should work with the PM to define "value" during the planning phase. Ideally, the definition of "value" and "measures of effectiveness[55]" should be included in the CNS. The USD(A&S) guidance supporting 5000.87 suggests the following examples:

- Increase in mission effectiveness
- Cost efficiencies
- User workload reduction
- User personnel reduction
- Equipment footprint reduction
- User adoption and user satisfaction.

If done properly, a value assessment requires capturing value data as a baseline before the implementation of the software to make the comparison post-implementation. This baseline data capture should be done on the legacy system (if one exists) before the development of the software system, as testers will be involved with testing the new system during development.

The OTA should work with the sponsor and user community to determine whether data they need to conduct the value assessment will need to be collected during operational testing, particularly in assessing the mission improvements and efficiencies realized. The OTA should incorporate collection of these data during OT&E events, as applicable. The OTA, sponsor, and user community should review the data collection needs at least annually to support the upcoming year's value assessment.

[54] DoDI 5000.82, page 8

[55] Note that these measures of effectiveness may not necessarily be the same as those developed by the OTA for OT&E. Value assessment measures of effectiveness may be more business related (e.g., cost reduction) than performance or mission effectiveness.

TEST AND EVALUATION CHAPTER 6: DEFENSE BUSINESS ACQUISITION

Table of Contents

1. Defense Business System (DBS) Acquisition Pathway Overview

1.1 Introduction

In accordance with DoDI 5000.02, the DoDI 5000.75 establishes policy for the use of the Business Capability Acquisition Pathway for business systems requirements and acquisitions. DoDI 5000.75 "applies to all defense business capabilities, including those with 'as-a-service' solutions such as financial and financial data feeder, contracting, logistics, planning and budgeting, installations management, human resources management, training, and readiness systems. It may also be used to acquire non-developmental, software intensive programs including national security systems, productivity solutions, and Information Technology (IT) infrastructure."[56] The guidance provided here supports policy established in the DoDI 5000.89 and DoDI 5000.75. In the event of conflict, the reader should defer to policy documentation.

Using the DBS Pathway to implement the Business Capability Acquisition Cycle (BCAC) processes, "functional leads and program managers will apply commercial best practices and lessons learned to prioritize and more rapidly develop and deploy useable, affordable subsets of capability."[57] The use of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) does not eliminate the need for independent government T&E. Integration of COTS into the DoD environment is not trivial, and development and test activities are still needed.

The Program Manager (PM) should involve the T&E organizations with the acquisition program from its inception and throughout its lifecycle to support program decisions and delivery timeline. Contractor testing (CT), developmental test and evaluation (DT&E), and operational test and evaluation (OT&E) should be integrated, streamlined, and automated to the maximum extent practicable to enable efficient use of data and resources across the test program and evaluation of system operational effectiveness, suitability, and cyber survivability to inform the decision authorities. Test and certification organizations should strive for maximum sharing, reciprocity, availability, and reuse of test results and artifacts. Collaboration between all organizations should be considered to develop digital system models, simulations, and test environments for common use across the spectrum of system tests that may produce necessary data or information.

1.2 Defense Business Acquisition Pathway Phases

Figure 1 illustrates the five major phases within the Defense Business System Acquisition pathways: 1) Capability Need Identification, 2) Solution Analysis, 3) Functional Requirements and Acquisition Planning, 4) Acquisition, Testing, and Deployment, and 5) Capability Support. The phases are separated by Authority to Proceed (ATP) decision points. These ATP decision points are informed by test measures and reports that assess the readiness to proceed to the next phase of the process. T&E community involvement in each phase is discussed in Section 2.

[56] DoDI 5000.02, 23 January 2020, p. 13
[57] DoDI 5000.75, January 24, 2020, p. 15

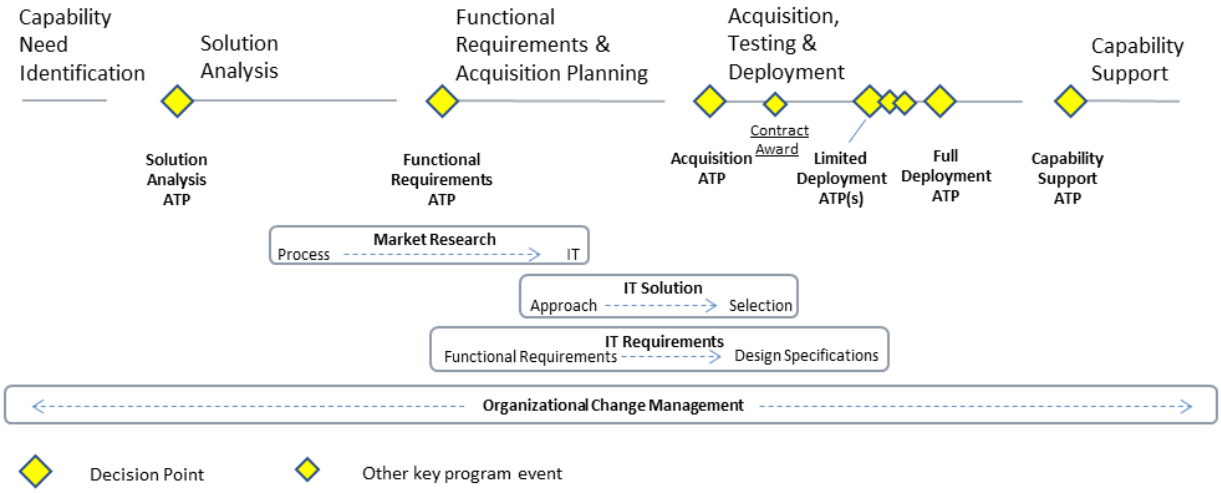


Figure 1. Business Capability Acquisition Cycle[58]

1.2.1 Capability Need Identification

The objective of the Capability Need Identification phase is to establish a clear understanding of needed business capabilities so that the functional sponsor and acquisition officials can decide to invest time and resources into investigating business solutions.[59]

During this phase, early capability requirements, attributes, and performance measures are developed. Capability requirements include prioritized business capabilities and their attributes, such as capability performance measures with associated threshold and objective values for capability performance.

Government test teams should be involved early in the program during this phase to understand the sponsor's functional needs and how they support the overall business operations. In this phase, the T&E community should ensure the testability of requirements and consider appropriate metrics for testing these requirements.

1.2.2 Solution Analysis

The objective of the Solution Analysis Phase is to determine the high-level business processes supporting the future capabilities to maximize use of existing business solutions and minimize creation of requirements that can only be satisfied by a business system."[60]

The Solution Analysis Phase begins with the Solution Analysis ATP, for which the appropriate decision authority, with input from the functional sponsor, validates the capability requirements, approves the work planned for the phase, and verifies the capability is aligned with the business enterprise architecture as well as organizational or OSD functional strategy and IT portfolio management goals. [61]

---

[58] DoDI 5000.75, January 24, 2020, p. 6
[59] DoDI 5000.75, January 24, 2020, p. 16
[60] DoDI 5000.75, January 24, 2020, p. 17
[61] DoDI 5000.75, January 24, 2020, p. 17

In this phase, the DT&E test lead and Operational Test Agency (OTA) should build an understanding of the planned business process changes for scoping test events through involvement in the business process change planning.

1.2.3 Functional Requirements and Acquisition Planning

The objective of the Functional Requirements and Acquisition Planning Phase is to establish the Acquisition Strategy and identify the capability support approach required to meet the functional requirements.[62]

The Functional Requirements and Acquisition Planning Phase begins with the Functional Requirements ATP, for which the appropriate decision authority validates that sufficient business process reengineering has been conducted to determine whether a business system is required, and the Milestone Decision Authority (MDA) approves execution of the activities outlined in the Capability Implementation Plan. [63] This ATP determines whether a business system will be acquired and begins the acquisition of that system.

The T&E community should be involved at this phase to ensure the testability of requirements, review the RFP for inclusion of T&E activities, and develop the initial Test and Evaluation Master Plan (TEMP), or other strategic document.

1.2.4 Acquisition, Testing, and Deployment

During this phase, the PM leads the execution of contract award, vendor management, establishment of baselines, delivery of the business system, and risk management. The functional sponsor leads training and deployment.[64]

Multiple ATPs and key events occur within this Phase:

- Acquisition ATP
- Contract Award
- Limited Deployment ATP
- Full Deployment ATP

Most DT and OT events and evaluations will occur during this phase.

1.2.5 Capability Support

The objective of the Capability Support Phase is to provide support for the business capability, including continued cybersecurity readiness and enduring support for appropriate upgrades to the business system.[65] At the Capability Support ATP, the functional sponsor accepts full deployment of the system and approves transition to capability support. During this phase, risk-based OT events and cyber assessments may be conducted.

---

[62] DoDI 5000.75, January 24, 2020, p. 18
[63] DoDI 5000.75, January 24, 2020, p. 18
[64] DoDI 5000.75, January 24, 2020, p. 19
[65] DoDI 5000.75, January 24, 2020, p. 20

1.3 Defense Business Systems T&E Overview

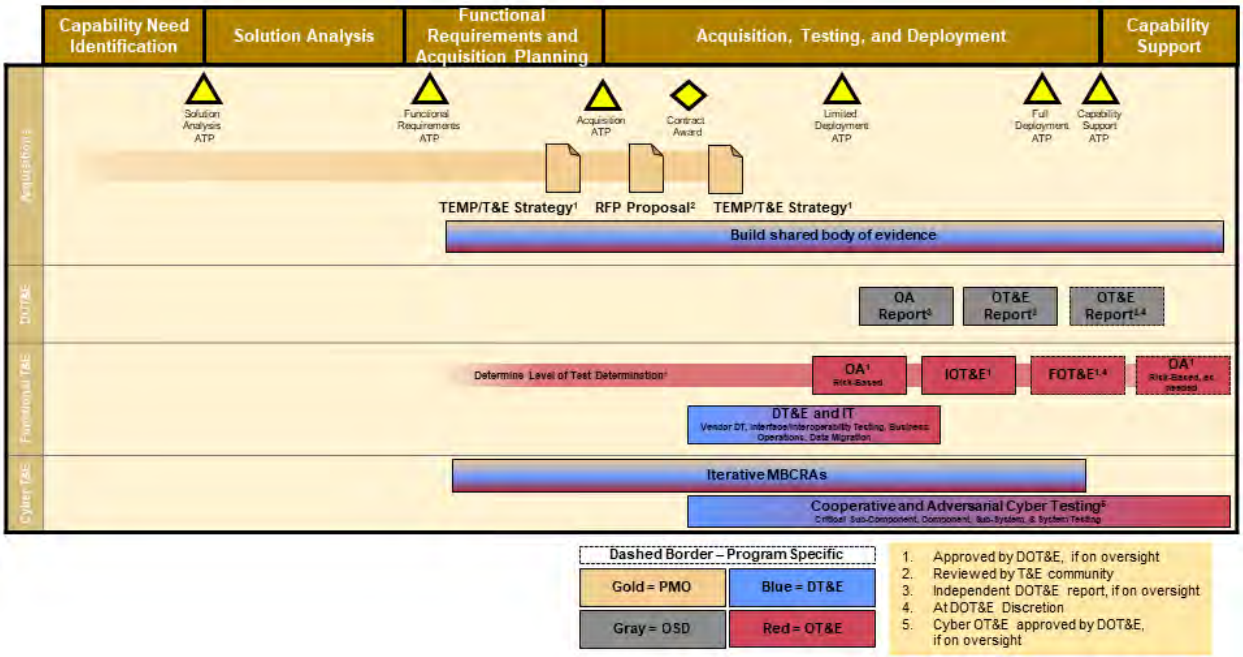


Figure 2. T&E Aligned with DBS Pathway

1.4 Test and Evaluation Working-level Integrated Product Team (WIPT)

The T&E WIPT should perform planning for all T&E-related products and events listed in Figure 2 and the integrated schedule, which should account for the time needed to fix any deficiencies identified in test, and the associated analysis, and reports. The T&E WIPT defines the data requirements and T&E resources needed to adequately plan and execute the T&E program. The PM, in coordination with the T&E WIPT, should ensure the T&E requirements are included in RFPs, and then the acquisition contract, to mitigate risk to the T&E program by gaining government access to necessary contractor data. In addition to contracts, the T&E WIPT should participate in acquisition program requirements refinement to ensure requirements are measurable, testable, achievable and relevant to the operational mission. The PM and T&E WIPT should coordinate with the requirements authority to clarify any requirements found untestable.

The T&E WIPT includes representatives from all organizations responsible for providing or overseeing the TEMP, or other strategic document, and its development and execution. In particular, the T&E WIPT should include representatives of test data stakeholders such as systems engineering, DT&E, OT&E, the functional lead,[66] interoperability evaluator, cybersecurity, product support, the Intelligence Community, and applicable certification authorities. The T&E WIPT should enable collaboration among stakeholders to maximize efficiency by planning and executing an integrated T&E program leveraging all test events for the purposes of meeting developmental and operational evaluation objectives. The PM should

[66] For a DBS program, the functional lead represents the functional sponsor (user), or DoD or component senior leader with business function responsibility seeking to improve mission performance.

ensure that results from all test events are captured in a shared data repository (discussed below) and available for all parties to use for independent assessment.

- Government test teams should be involved from the inception of the program to ensure their T&E requirements are captured in acquisition contacts and that they have a process to generate the required data.
- Government test teams should strive to maintain a tempo that supports the required decisions using various tools (e.g., digital engineering, sequential testing, automation).
- Government test teams should develop a robust T&E program to support the ATP decisions with end-to-end mission threads employing actual users.
- OT&E should concentrate on appropriately scoped, dedicated tests while integrating useable data and information from all sources to meet stakeholder needs, support operational evaluations, and inform decisions.
- The T&E WIPT may develop collaborative test data scoring boards to evaluate and authenticate any available test data for potential to meet any IOT&E requirements.

Embedding OT&E earlier in the program's lifecycle requires OT&E awareness and participation in the system engineering and system development. This includes monitoring the tests that occur throughout the development and understanding and trusting the veracity of the developmental testing to determine which results may be usable for operational evaluation. The test community should determine the applicability of prior data for OT&E, including the mapping of that data to the evaluation assessment areas, and identify gaps in data that will inform test planning for future iterations.

User involvement is critical for DBS testing. Some DBS programs have a user organization, often referred to as the Functional Sponsor, at a level equal to the Program Management Office (PMO), to manage requirements, assist in software development, and support T&E, while others may have user organizations with less influence over system development. In any case, the test lead should work to incorporate these user organizations into the test strategy. When functional users are working with the operational system, the OTA should work with the PMO to gather relevant information such as deficiencies, software trouble tickets, and other available system performance observations to support test reporting. The T&E Lead, OTA, and T&E WIPT should work closely with the Functional Lead to ensure users are available for mission-oriented DT and OT, respectively.

1.5 Test and Evaluation Planning for Defense Business Systems Pathway

The purpose of the T&E planning is to better understand users' needs and plan the approach to credibly demonstrate the technical, functional, and operational capabilities that need to be delivered to meet users' needs. As the planning process is critical and sets the conditions for success, all test teams should be involved early to establish and document how testing, modeling and simulation (M&S), analysis, and evaluation of system performance at its various maturity stages will be accomplished. The T&E WIPT should identify the measures to evaluate the system, and then the data needed and conditions under which those data will be collected. A tabletop exercise can assist in confirming the feasibility of the proposed plans, tools, and methodology.

Testing and planning should be digitized and automated as much as possible to support continuous development, integration, and delivery of system capabilities. Digital test

management tools automate the process of test planning, scheduling, tracking, and reporting test events.

During the planning process, various stakeholders are developing documentation, summarized and defined in Table, to include the associated testing resources, tools, data and infrastructure.

Table 5. Planning Documents

Artifact	Description	Developed by
Test and Evaluation Master Plan (TEMP), or other strategic document	Defines the processes by which technical, functional, and operational performance will be tested and evaluated to satisfy developmental T&E criteria and to demonstrate operational effectiveness, suitability, and cyber survivability.	Program Manager with support from T&E WIPT
Functional Requirements	Specifies the functional requirements for the system that will support the business processes.	Sponsor with support from the Program Manager
Capability Implementation Plan (CIP)	Aggregates the content needed to prepare for and manage the delivery of the capability to support statutory and regulatory requirements. It is not a specific document or set of documents, and accounts for all necessary information products required to support and inform leadership decisions.	Program Manager
Cost Estimate	Developed in accordance with DoDI 5000.73 (Cost Analysis Guidance and Procedures). The estimate should consider the technical content of the program and test strategy.	Program Manager
Request for Proposals	A document used in negotiated acquisitions to communicate government requirements, including those for T&E, to prospective contractors, and to solicit proposals.	Program Manager

1.5.1 Test and Evaluation Master Plan

The TEMP, or similar strategic document, serves as an agreement between the PM and all the T&E stakeholders for the T&E program, including T&E roles and responsibilities, and resources. The TEMP captures the data requirements and processes by which the system will be tested and evaluated to verify technical requirements and to evaluate operational effectiveness, suitability, and cyber survivability. The TEMP should enable the evaluation of the user equipped with the system executing the missions the system is intended to perform while considering all interfacing systems, threats, and operational environments. In particular, the T&E WIPT should consider all possible cyber-related threats necessary to assess cyber survivability in a mission context.

The T&E WIPT should ensure the TEMP, or similar strategic document, is executable and aligns with the Acquisition Strategy, T&E policy (DODI 5000.89), and relevant T&E focus area chapters in the T&E Enterprise Guidebook. Per the DoDI 5000.89, the TEMP, or similar strategic document, should include an Integrated Decision Support Key (IDSK), a table outlining the acquisition, technical, and program decisions as well as the data (e.g., CT, DT, OT) necessary

to support those decisions. The IDSK provides a framework for how test events can build on one another and support the data requirements for multiple stakeholders' evaluations simultaneously, producing efficiencies across the T&E lifecycle and facilitating the integration of DT, CT, and OT. The IDSK should evolve and adapt as the system matures and identify opportunities to incorporate operational realism (e.g., mission environments and operational users) as early as possible. Incorporating operational realism early in the test program improves the probability of identifying and correcting problems early, rather than later in development when redesigns are more expensive and correcting the problem may prove infeasible. This approach does not support the replacement of dedicated DT&E or OT&E, but may affect the scope of individual test events if stakeholders can pull data from prior events to support their evaluations. The TEMP should describe how these data will be collected to build a shared body of evidence to support evaluations of the system during the various acquisition phases.

The TEMP should define the conditions under which required data will be collected, and any tools required to manage the data and perform the testing. OT should consider informing the DT community of their OT data requirements to meet their evaluation objectives, and vice versa. As such, DT should consider the operational relevance of the developmental tests to identify operationally representative deficiencies sooner in the acquisition cycle.

The strategy for testing DBS should consider data collected from both external sources and independent government testing. Testing should emphasize mission performance, specific task completion, and usability, while employing actual operators when possible (especially in Integrated Testing and dedicated OT), end-to-end scenarios, and live interfaces or representations of interfacing systems if live interfaces are not available or feasible. Backend or non-functional capabilities should also be tested (e.g., data backup, load balancing, system failover).

For programs on OSD T&E oversight, a TEMP is required and DOT&E is the final approver for the TEMP.[67] At specified milestones, the TEMP is submitted to the Director for approval no later than 45 calendar days before the supported decision point. To support agile acquisition, the timeline for TEMP delivery may be tailored with mutual consent by DOT&E, the OTA, and Program Office. Programs not under DOT&E oversight are encouraged to develop a TEMP or similar strategic document as a component of the CIP. Whether it is a section of the CIP or a separate TEMP, the test planning document should be sufficient to support the detailed planning, execution, and reporting of test events and, at a minimum, be approved by senior leadership of the stakeholders. The MDA is the approval authority for the DT&E plan in a Business Systems Category (BCAT) I TEMP, or similar strategic document. The TEMP should be updated as new data are collected and as the program reaches new acquisition milestones and decision points.

a. T&E Resources

The TEMP, or similar strategic document, should document the T&E resources required to support DT&E and OT&E. Programs should identify one-of-a-kind T&E resources and long-lead items early in the acquisition process to allocate adequate funding for development and use. The lead test organizations should verify and validate the test infrastructure and tools planned for

[67] DoDI 5000.89, November 19, 2020, pg. 5

OT&E to support acquisition decisions. This verification and validation should consider data collection, interfacing systems and databases, networks, simulated environments, simulated users, and ranges. The commitment to provide a verification and validation plan for each tool or test infrastructure asset should be documented in the TEMP, or similar strategic document. The TEMP, or similar strategic document, should specify when particular T&E resources are required, and which organization is responsible for providing the associated resources.

These resources may include, but are not limited to:

1) **Test articles (e.g., the system under test, interfacing systems, and cyber threats)** The environments used to conduct testing for OT&E should represent the operationally realistic environment as closely as possible, including realistic system use and cyber threats. This requires the interfacing systems that form the system of systems with the program of record.

2) **Test facilities, infrastructure, instrumentation, and ranges, to include cyber ranges and test team, software integration laboratories.**

Programs should use government T&E capabilities unless an exception can be justified as cost-effective to the government. PMs will conduct a cost-benefit analysis for exceptions to this policy and obtain approval through the TEMP approval process before acquiring or using non-government test facilities or resources.

The TEMP should include any proposed use or application of embedded instrumentation. The intent of embedded instrumentation is to facilitate data collection and system diagnostics without modifying the system's operational configuration. The PM, in coordination with the T&E WIPT and other stakeholders, should plan for the use of embedded instrumentation to collect system performance and diagnostic data whenever feasible, and should work together to obtain accreditation and certification prior to use in OT&E. This may include adding requirements for these embedded instrumentation in programs RFPs and other resourcing provisions.

3) **Automated testing tools**

Automated test execution tools should be part of the process of executing test cases or procedures on the system under test. The T&E WIPT and PM should work with the contractor to fully understand contractors' tools, specifically their verification and validation plans, and the credibility of those tools for the intended use. The automated tools should also provide visibility into the continuous testing occurring within the development process so that stakeholders can gain confidence on the quality of the development process. The government test teams should be knowledgeable about all these tools as appropriate so they can use their outputs to inform evaluations. Using the same tools as the contractor is advantageous for the government (e.g., easier to replicate events when necessary) and should be included in the acquisition contract. In some cases, government test teams may need to become experts in the tools used by both the contractor and government. Such expectations should be clarified within the appropriate contractual provisions.

(4) **M&S, and their verification and validation plans**

The TEMP should document initial and subsequent versions of system M&S tools to be matured during development for use by government test organizations during Engineering &

Manufacturing Development (EMD) and beyond. These may include initial digital system models, component-level reliability and availability models, or other M&S tools. The PM, in collaboration with the T&E WIPT, should also consider whether the delivery of these tools, when applicable, should be included in the program RFPs.

The M&S strategy and schedule, including the using organization, intended use, and the commitment to provide a verification and validation plan for each tool or test infrastructure asset, should be documented in the TEMP. The TEMP should specify when particular T&E resources are required, and which organization is responsible for verification and validation, and for providing the associated resources.

5) **Manpower and personnel**

The TEMP should include information about friendly and cyber threat operational forces, data collectors, and subject matter experts that will be required to execute the T&E program.

6) **Federal/State/local requirements, range requirements, and any special requirements**

This may include requirements for frequency management and control.

7) **Projected and actual level of funding**

Pursuant to Section 839(b) of Public Law 115-91, the PM should include a table in the TEMP, or similar strategic document, listing the initial resource estimates for DT&E and OT&E, which should be updated each time the TEMP or similar strategic document is updated. T&E funding in the resources section should be consistent with the cost estimate and budget submissions.

8) **Shared Body of Evidence and Data Repository**

At program initiation, the PM should establish a shared data repository to store test and evaluation data and provide access to all test teams so they can review, use, and input these test data to meet their objectives. This should enable the use of sequential testing, big data analytics, and other adaptive methods in support of T&E efficiencies. Throughout system development, T&E should be building a shared body of test evidence to support efficient technical, functional, and operational performance evaluations and adaptive T&E. Relevant test data gathered through all testing should be included in this test data repository. To enable adequate use of sequential testing and similar T&E planning and analysis methods, the T&E WIPT may leverage existing or develop collaborative test data scoring boards to evaluate integrated test data for potential to meet IOT&E data requirements. The OTA should maintain the record of authoritative data that may meet requirements for inclusion in OT&E.

1.5.2 T&E Content and Interests in Other Planning Documents

While the TEMP, or similar strategic document, is the main testing deliverable, the success of T&E relies heavily on each of the other documents outlined in Table. The T&E community should work with the acquisition community on these documents to incorporate needed T&E

information. This section highlights T&E content and involvement of test teams in the development of each of these documents.

1.5.2.1 Functional Requirement

Testers should work with the system engineer to sort out the hierarchy of requirements and capture them in a way that can trace requirements from the highest-level capabilities to the testable requirements, and to the test events that verify and validate their satisfaction. This includes cyber survivability requirements, whether stated, implied, or derived. The test strategy should capture the key capabilities to focus testing priorities. Equally important are the interoperability needs to start planning for interoperability testing. DoDI 5000.75 does not define a specific requirements document, but discusses needed business capability requirements, capability attributes, performance measures, IT functional requirements, and design specifications.

1.5.2.2 Capability Implementation Plan

The DBS uses the Capability Implementation Plan (CIP) as the major planning document, and the TEMP or similar strategic document is part of the technical management content within the CIP. DoDI 5000.75 notes that "Information requirements will generally not be prepared solely for staff review and approval. In addition to supporting decision-making at ATP decision points, these products should support program activities such as contracting actions or test events, or serve as planning and management tools. The information produced will be specific to each program and acquisition information (e.g., acquisition strategy content) will be tailored to meet individual program needs. Details will be maintained by the program in a transparent and timely manner, readily available for reviews as needed."

1.5.2.3 Cost Estimate

The cost estimate should consider the technical content of the program described in the requirements, Acquisition Strategy, and TEMP, or similar strategic document. Test teams should ensure that the cost estimate includes all the resources necessary to plan and execute the T&E as outlined in the TEMP, or similar strategic document, including cyber T&E, and resources to mitigate potential deficiencies identified in test.

1.5.2.4 Request for Proposal (RFP)

The RFP defines what the government expects from the contractor. T&E expectations should be explicitly stated in the RFP to reduce risk to the T&E program and potentially the acquisition cost and schedule. The TEMP, or similar strategic document, is a source document for the RFP and needs to be generated in time to support the RFP development. The PM should consult with government test teams to ensure that the RFP supports data collection for government T&E. At a minimum, a draft TEMP or similar strategic document should be included as an attachment to the RFP to clearly tell the contractors what the government intends to test and evaluate. The test teams should encourage the inclusion of the following items and activities as contract deliverables:

- Government access to contractor test events, test tools, test data repositories, and test environments
- Contractor test plans, procedures, reports, and data

- Contractor support for Government testing

2. T&E During Defense Business Systems Pathway Phases

2.1 Capability Need Identification Phase

There are no specific T&E activities within this phase. Testers should be involved to understand functional sponsors' needs and how they support the overall business operations. Testers may help guide requirements development to ensure testability and provide input into metrics for testing requirements.

2.2 Solution Analysis Phase

Specific T&E activities within the Solution Analysis Phase should include providing input to initial CIP development. The T&E community should be involved early in the development and review of information requirements within the CIP that will directly support DT&E and OT&E.

2.3 Functional Requirements and Acquisition Planning Phase

Specific T&E activities within the Functional requirements and acquisition planning phase include:

- Ensure the testability of functional and non-functional requirements
- Participate in RFP development
- Generate the initial TEMP, or similar strategic document

2.3.1 Ensuring the testability of functional and non-functional requirements

The T&E community should be involved in the development of functional requirements throughout this phase to ensure they are clearly stated and testable, as they form the foundation for test planning. DoDI 5000.75 states that the functional requirements describe how the business system will achieve the future business processes; include enough detail to inform definition of potential business system solutions and evaluation criteria, but not too much detail that would overly constrain solution selection; and will be linked to inputs and outputs that define how the functional requirements support the business processes.

The linking of the functional requirements to business processes allows the testers to develop mission-oriented test events with end-to-end mission threads. Although unstated, users and testers should also be involved and support the development of non-functional requirements such as availability, performance measures (e.g., latency, maximum loading), and cyber survivability. Testers should be deeply involved in requirements development.

2.3.2 Participating in RFP development

Testers should request that any contractor support for testing is included in the RFP and the initial test plan is included in the RFP to inform vendors of the overall test strategy. The T&E Lead should ensure appropriate environments are available to support testing (typically: developmental, testing, pre-production, production). The RFP should allow government testers access to vendor testing, vendor environments for cyber survivability testing, to include cloud application hosting and data storage sites, and vendor test planning and data to allow the overall combined and integrated testing to share test data.

2.3.3 Generating the initial TEMP, or similar strategic document

The content should be tailored based on known information about the DBS solution prior to contract award. PMs and OTAs should coordinate with DOT&E on TEMP content that cannot be addressed prior to contract award, such as failure definitions and change management metrics.

The TEMP should be updated as appropriate to include exit criteria from developmental testing to lead to a limited deployment of the system for operational testing and limited operational use. Typical criteria may include that the developer has corrected all defects that affect the ability of users to accomplish critical functions, with approved workarounds for any less critical defects not remediated before deployment. The TEMP should also include operational testing entrance criteria such as all test participants are trained cyber defenders, and help desk personnel are trained and available, and all required system documentation is available to system users and maintainers to support mission accomplishment.

2.4 Acquisition, Testing, and Deployment Phase

Specific T&E activities within the Acquisition, Testing, and Deployment phase include:

- Support the Acquisition ATP
- Support the contract award
- Conduct DT&E to support the limited deployment ATP
- Conduct OT&E to support the limited deployment ATP
- Conduct DT&E to support the full deployment ATP
- Conduct IOT&E to support the full deployment ATP
- Participate in TEMP, or similar strategic document, updates, as appropriate
- Plan and conduct FOT&E, if necessary

2.4.1 Support the Acquisition ATP

For the Acquisition ATP, the MDA verifies the requirement is fully funded across the Future Year's Defense Program to support all the acquisition activities requested for approval, authorizes execution of the Acquisition Strategy, and approves continued execution of the CIP.[68] The PM will prepare an initial TEMP or similar strategic document to support the Acquisition ATP decision with input from the T&E WIPT[69].

2.4.2 Support the Contract Award

While the PMO is responsible for providing the RFP, the test organizations should review the proposed scope of the contract to ensure they understand the potential level of effort and proposed timelines the PMO is submitting for bid. Testers should ensure that the RFP and subsequent contract contain provisions stipulating that:

- Government testers have access to vendor testing, including test data and reports
- Contractors are required to fix mission-critical findings before government acceptance testing

[68] DoDI 5000.75, January 24, 2020, p. 19
[69] Capability Implementation Plan Information Requirements, Table 6 of DODI 5000.75

- The government has the authority to send the DBS solution back to the contractor if mission-critical findings are not mitigated to an acceptable level

The RFP and subsequent contract should also contain provisions for:

- Contractor-led, mission-based, cyber risk assessments
- Vendor tasks to support government testing
- Accesses for government cyber T&E activities, as required

2.4.3 Participate in TEMP, or Similar Strategic Document, Updates

The PMO should update the TEMP, or similar strategic document, following contract award and when the program reaches new acquisition decision points. For the Limited Deployment ATP(s), Full Deployment ATP, and subsequent decision points, the MDA, the senior DoD Component leadership, or DOT&E (for programs on T&E oversight) may require TEMP updates or addendums to address changes to planned or additional testing.

After the PMO awards the acquisition contract, the prime contractor, and sub-contractors, if applicable, will provide detailed delivery schedules to the PMO. These detailed schedules will provide a baseline for a TEMP update to reflect the proposed timelines and actions for the acquisition. The testing, user, and acquisition communities should also update system documentation to reflect any requirement changes after contract award.

As a DBS, the system contracted by the PMO may be mainly COTS or GOTS software, custom coded software, or a combination of off-the-shelf and custom code, to include Reports, Interfaces, Conversions, Extensions, and Forms and Workflows. Along with updates to schedules and evaluation plans, additions to the TEMP to address these items include:

- Failure Definition and Scoring Criteria (FDSC) that allows categorization of the defect cause (hardware, software, user error, etc.), what is considered a failure that effects system availability, what constitutes a system downing event and associated restoral activity, what failure(s) constitute a mission failure
- Defect severity definitions (e.g., IEEE Standard 12207.2, Annex J)
- Metrics to determine the maturity of the software (e.g., defect aging, defect density, and function point analysis)
- Metrics for evaluating Change Management and Business Process Reengineering needed to adopt the business processes inherent in the proposed acquisition
- Hosting solution and cloud service provider

2.4.4 Conduct DT&E to Support the Limited Deployment ATP

DT supporting the Limited Deployment ATP and all subsequent deployment decisions may include the following:

- Mission-based cybersecurity risk assessments among the vendor, Program Office, government testers, cyber blue and red teams, and cyber defenders. This is conducted early, as soon as the vendor has a system concept with defined attack surfaces to focus subsequent cybersecurity testing.

- Vendor DT: Includes unit testing at the developmental team and system integration testing among software units and functions
- Interface testing between the DBS and other systems that the DBS must interoperate with. The T&E Lead should start before this phase to arrange test environments to conduct testing. Interface testing should evaluate both the exchange of data and the processing of the data on both systems.
    - Interoperability DT&E will include testing with actual representations of interface systems in a controlled environment. DT with the test environments of the interfacing systems is preferred, if available. This takes advance planning. Interoperability testing on production environments is limited by the risk of test actions accidently making real-world transactions or corrupting operating data bases.
- Cybersecurity vulnerability identification (CVI) includes multiple activities for the early identification of vulnerabilities (e.g., supply chain assessment and cooperative vulnerability assessments with blue teams). See Cyber T&E Companion Guide for more information.
- Data migration testing: If the DBS replaces a legacy system and data within the legacy system will be migrated to the new DBS, migration testing is needed to assess the effective, accurate, and complete migration capability.
- Business operations testing (BOT). This is a form of mission-oriented DT where actual users perform scripted business operations in the test environment. As the testing progresses, users have more free play to perform their business operations. This may be the culmination of DT and can evaluate end-to-end mission thread performance, human-systems interface, training documents, and initial user feedback. While this is a DT event, it is critical to include the OTA, as data collected may support future operational assessment and evaluation. The T&E Lead should consider the following during this test:
    - Sufficient mission-threads to exercise all functional requirements (including those that may be exercised infrequently, such as year-end close out)
    - Including interfacing systems or accredited simulations to represent the interfacing system
    - Test data sets to populate the DBS with expected business data
    - Potential test loading to evaluate scalability
- Adversarial Cybersecurity DT (ACDT), which may be conducted concurrent with the BOT, incorporates users performing business operations with red teams and cyber defenders.
- Scalability testing includes the use of automated tools to replicate the impact of increasing user population, addressing one of the common problems of business systems: performance when the user population increases to tens of thousands of users.

Based on the Acquisition Strategy, DBS programs may have multiple Limited Deployment ATPs. The same DT&E should be applied as appropriate to each Limited Deployment ATP. At the Limited Deployment ATP decision point, the MDA, in conjunction with the functional sponsor, considers the results of testing indicating adequate performance and cybersecurity, and approves deployment of the release to limited portions of the end user community. Multiple

limited deployments may be authorized at the same decision point or delegated to a lower decision authority.

2.4.5 Conduct OT&E to Support the Limited Deployment ATP

Limited deployment could include all system capabilities to a small set of users or a small set of capabilities to a large user base. Prior to the Limited Deployment ATP decision, and based on the proposed definition of limited deployment, the OTA will perform a risk assessment based on the latest DOT&E and Service guidance to determine the appropriate level of OT to support the Limited Deployment ATP. The risk assessment may include operational risks generated by the content (size) of the deployment, the number of users affected, the risk to operations if the deployment fails, and other considerations as outlined in the memorandum.

The level of test determination should also consider the decision, if any, that the testing will support. The OTA should submit the risk assessment and level of test determination to DOT&E for approval, and refine the operational test plan accordingly based on the approved level of test.

The test plan should include details on specific data collection, data evaluation, and reporting required to determine progress toward operational effectiveness (including interoperability), suitability, and cyber survivability if the test is Level 2 or below. If the test is Level 3, the data collected and evaluated should be sufficient to fully determine operational effectiveness (including interoperability), suitability, and cyber survivability.

The OTA should conduct risk assessments for subsequent Limited Deployment ATP(s) and execute operational testing and evaluation at the level determined through those risk assessments to support those ATP(s).

2.4.6 Conduct DT&E to Support the Full Deployment ATP

The DT&E team should prepare a consolidated summary DT report to present at the Initial Operational Test and Evaluation (IOT&E) Operational Test Readiness Review. In some cases, additional DT&E may be required following the IOT&E to verify correction of defects found during IOT&E.

At the Full Deployment ATP decision point, the MDA, in conjunction with the functional sponsor and appropriate CMO decision authority, considers the results of limited deployment(s), the results of indicating adequate performance and cybersecurity, and operational testing, and approves deployment to the entire user community.

2.4.7 Conduct IOT&E to Support the Full Deployment ATP

The OTA must execute an IOT&E event to support the Full Deployment ATP decision using a DOT&E-approved test plan, as described in the DoDI 5000.75. By definition, the IOT&E is a Level 3 test event, so the OTA does not need to perform a formal risk assessment and level of test determination.

The PMO, OTA, and users should develop a set of entrance criteria, codified in the TEMP, delineating the necessary conditions that the system maturity and test and user personnel training and availability should meet to proceed to Full Deployment ATP decision and subsequent deployment and testing activities. These conditions could require further DT or regression

testing, modification to training plans, and other activities required to ensure the system is mature and ready for operational use.

The results of the OT may include the discovery of latent defects and faults in the system software, deficiencies in user training and system documentation, inadequate help desk support, change management and configuration management problems, and other issues that impact the user's ability to complete their missions. Based on the problems that the testers discover in the IOT&E, the developer may need to remediate some or all problems before further deployment of the system with additional capabilities, additional users, or both. For systems on DOT&E oversight, an IOT&E report is required prior to the full deployment ATP.

2.4.8 Plan and Conduct FOT&E, If Necessary

If directed by DOT&E, the OTA will execute a Follow-on OT&E (FOT&E) event after full deployment is approved, but before entering the Capability Support phase. The FOT&E should ensure the system is operationally effective, suitable, and cyber survivable, and supportable in accordance with the system lifecycle sustainment plan or similar logistics support documentation.

2.5 Capability Support Phase

During this phase, risk-based operational events (e.g., OAs) and cyber assessments should be conducted as needed.