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

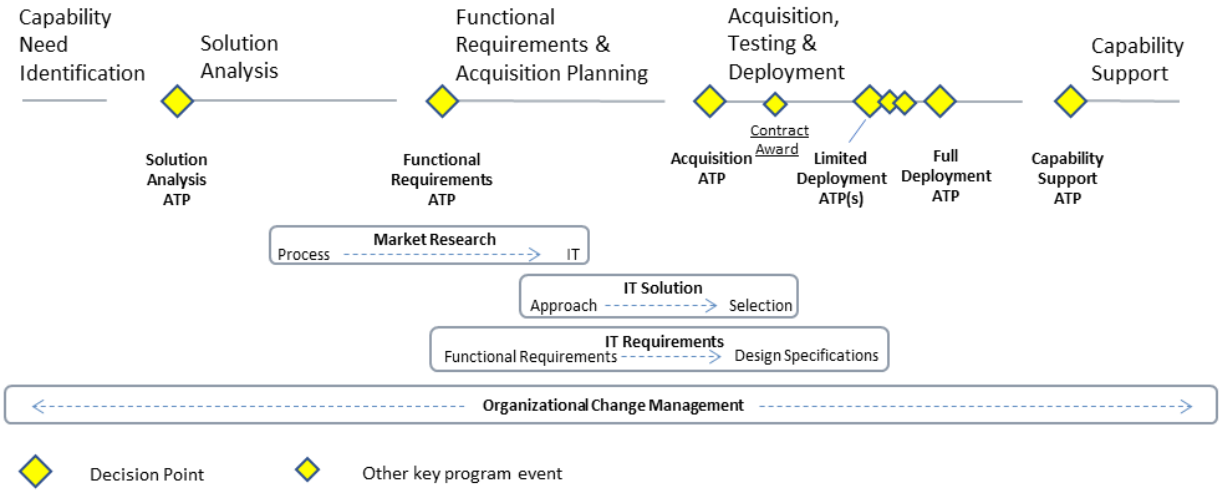

Figure 1. Business Capability Acquisition Cycle[58]

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

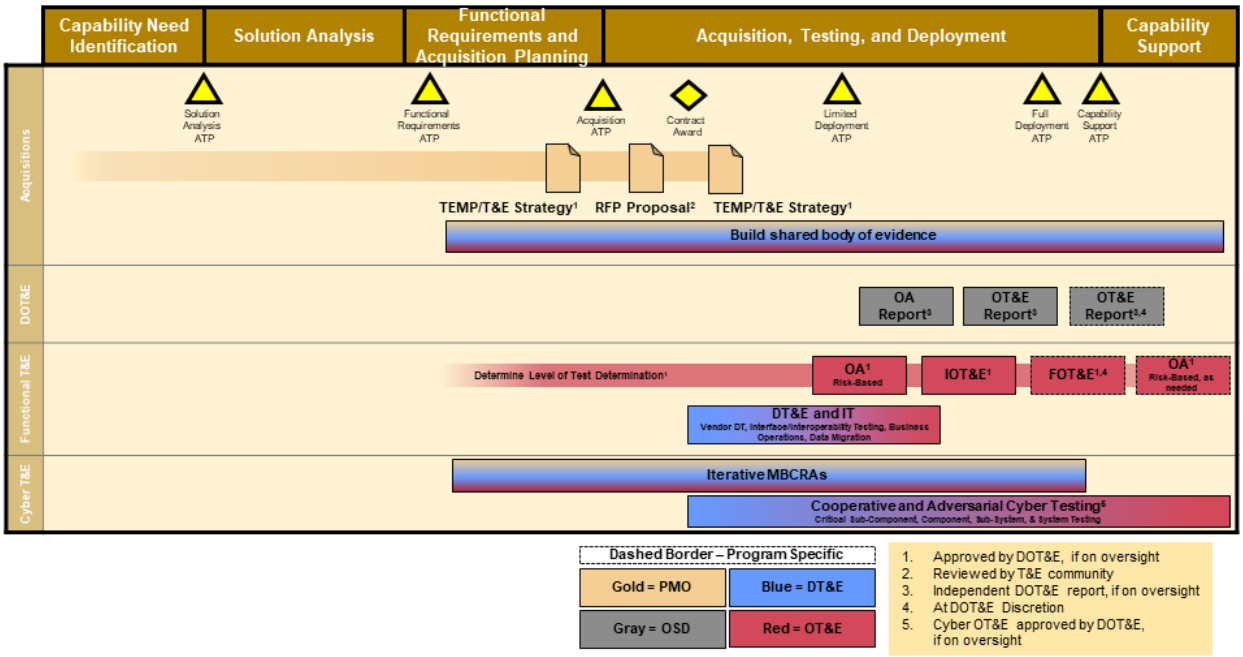

Figure 2. T&E Aligned with DBS Pathway

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.