DoD Instruction 5000.89

Test and Evaluation

Originating Component:	Office of the Under Secretary of Defense for Research and Engineering
Originating Component:	Office of the Director, Operational Test and Evaluation
Effective:	November 18, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Enclosure 4 and Enclosure 5 of DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended
Approved by:	Michael J.K. Kratsios, Acting Under Secretary of Defense for Research and Engineering
Approved by:	Robert F. Behler, Director, Operational Test and Evaluation

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02 and DoDD 5141.02, this issuance establishes policy, assigns responsibilities, and provides procedures for test and evaluation (T&E) programs across five of the six pathways of the adaptive acquisition framework: urgent capability acquisition, middle tier of acquisition (MTA), major capability acquisition, software acquisition, and defense business systems (DBS). The sixth pathway, defense acquisition of services, does not require T&E policy and procedures.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

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

1.2. POLICY.

a. The DoD Components will:

(1) Conduct developmental T&E (DT&E), operational T&E (OT&E), and live fire T&E (LFT&E) as part of an adequate T&E program.

(2) Integrate test planning and test execution across stakeholders to facilitate an efficient use of data and resources.

b. For non-major defense acquisition programs (MDAPs) and for programs not on T&E oversight, these guiding principles should be used as a best practice for an integrated and effective T&E strategy.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR OF OT&E (DOT&E).

Pursuant to Section 139, Title 10, United States Code (U.S.C.), 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 in the DoD, and the principal OT&E official within the senior management of the DoD. The DOT&E:

a. Prescribes policies and procedures for the conduct of OT&E and LFT&E for the DoD across the acquisition pathways.

b. Monitors and reviews OT&E and LFT&E activities in the DoD.

c. Oversees MDAPs or other programs designated by the Director.

d. Determines specific OT&E and LFT&E policy and best practices for each of the acquisition pathways as applicable.

e. Designates select programs for DOT&E operational and live fire oversight in accordance with Sections 139, 2366, 2399, and 2400 of Title 10, U.S.C., as applicable, and the criteria outlined in Paragraph 3.2 of this issuance.

f. Publishes and manages the T&E oversight list, which identifies all programs under oversight for DT&E, OT&E, or LFT&E.

g. Approves the OT&E and LFT&E planned activities in test and evaluation master plans (TEMPs), test strategies, or other overarching program test planning documents for programs on the T&E oversight list.

h. Approves, in writing, the adequacy of operational test (OT) plans for those programs under DOT&E oversight before OT begins.

i. Approves LFT&E strategies and waivers before LFT&E activities begin and in accordance with the timeline established in Section 2366 of Title 10 U.S.C.

j. Determines the quantity of articles to be procured for OT for systems on the T&E oversight list.

k. 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.

l. Assesses the adequacy of OT&E and LFT&E performed by the Military Services and operational test agencies (OTAs) for programs under T&E oversight.

m. 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.

n. Submits independent OT&E and LFT&E reports to the OSD, Joint Staff, DoD Components, and congressional defense committees, as applicable.

o. Submits a report after the conclusion of OT&E, as required by Section 2399 of Title 10, U.S.C., to the OSD, Joint Staff, DoD Components, and congressional defense committees before systems under T&E oversight may proceed to beyond low-rate initial production (LRIP).

p. 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 Section 139(h) of Title 10, U.S.C.

2.2. USD(R&E).

Pursuant to Section 133a of Title 10, U.S.C. and DoDD 5137.02, the USD(R&E):

a. 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.

b. Prepares Milestone B (MS B) and Milestone C (MS C) DT&E sufficiency assessments on those MDAPs where the Defense Acquisition Executive (DAE) is the milestone decision authority (MDA).

c. Develops DT&E policy and ensures appropriate test facilities, test ranges, tools, and related modeling and simulation capabilities are maintained within the DoD.

d. 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 concepts of operations.

e. Approves the DT&E plan within TEMPs and delegates approval authority, as appropriate.

f. Develops governing policy and advances practices and workforce competencies for DT&E.

SECTION 3: T&E PROCEDURES

3.1. OVERVIEW.

a. The fundamental purpose of T&E is to enable the DoD to acquire systems that support the warfighter in accomplishing their mission. To that end, T&E provides engineers and decision-makers with knowledge to assist in managing risks; to measure technical progress; and to characterize operational effectiveness, operational suitability, interoperability, survivability (including cybersecurity), and lethality. This is done by planning and executing a robust and rigorous T&E program.

b. Integrated testing and independent evaluation are part of a larger continuum of T&E that includes DT&E (both contractor and government), OT&E, and LFT&E. Integrated testing requires the collaborative planning and execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders. Whenever feasible, the programs will conduct testing in an integrated fashion to permit all stakeholders to use data in support of their respective functions.

c. Programs will incorporate integrated testing at the earliest opportunity when developing program strategies, plans with program protection, documentation, and T&E strategies or the TEMPs. Developing and adopting integrated testing early in the process increases the effectiveness and efficiency of the overall T&E program.

(1) If done correctly, integrated testing provides greater opportunity for early identification of concerns to improve the system design, and guides the system development during the engineering and manufacturing development phase. Conducting critical test activities earlier will enable the discovery of problems that the program can fix while the system is still in development and avoid costly redesigns late in the acquisition life cycle.

(2) Integrated testing and independent evaluation also encourage the sharing of all developmental test (DT), OT, and live fire test resources to accomplish the test program. For programs informing decisions that are not addressed in Title 10, U.S.C., such as fielding, deployment, and low-rate production decisions, well planned and executed integrated testing may provide necessary data for an OTA to determine the system's operational effectiveness, suitability, and overall mission capability.

(3) Integrated testing does not replace or eliminate the requirement for IOT&E, as a condition to proceed beyond LRIP for programs with beyond low-rate (i.e., full-rate) production decisions as required by Section 2399 of Title 10, U.S.C.

d. To ensure T&E focuses on informing the program's decision-making process throughout the acquisition life cycle, the TEMP will include the program's key decision points and the T&E information needed to support them. These decisions may be made by leaders ranging from the program manager (PM) to the MDA, and should represent major turning or decision points in the acquisition life cycle that need T&E information in order to make an informed decision. Examples include milestone decisions, key integration points, and technical readiness decisions.

This information is captured in a table known as the Integrated Decision Support Key (IDSK). This table is developed by the PM by analyzing what is already known about the capability, what still needs to be known about the capability, and when it needs to be known.

e. The PM:

(1) Resources and executes the system's integrated test and independent evaluation program.

(2) Identifies DT, OT, and LF data requirements necessary to support decisions, in consultation with the chief developmental tester (CDT), the chief engineer, and the OTA representative, and combines them into an IDSK.

(3) Charters an integrated test planning group (i.e., the T&E Working-level Integrated Product Team (WIPT), also known as an integrated test team) early in the program. It will consist of empowered representatives of test data producers and consumers (including all applicable stakeholders) to ensure collaboration and to develop a strategy for robust, efficient testing to support systems engineering, evaluations, and certifications throughout the acquisition life cycle.

f. The T&E WIPT, chaired by the CDT:

(1) Provides a forum for involvement by all key organizations in the T&E effort.

(2) Develops the TEMP for the PM. Requires all key stakeholders to be afforded an opportunity to contribute to TEMP development.

(3) Includes 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.

(4) Supports the development and tracking of an integrated test program for DT, OT, LFT&E, and modeling and simulation to support evaluations.

(5) Supports the development and maintenance of the integrated test schedule.

(6) Identifies and provides a recommended corrective action or risk assessment.

(7) Explores and facilitates opportunities to conduct integrated testing to meet DT, OT, and LFT&E objectives.

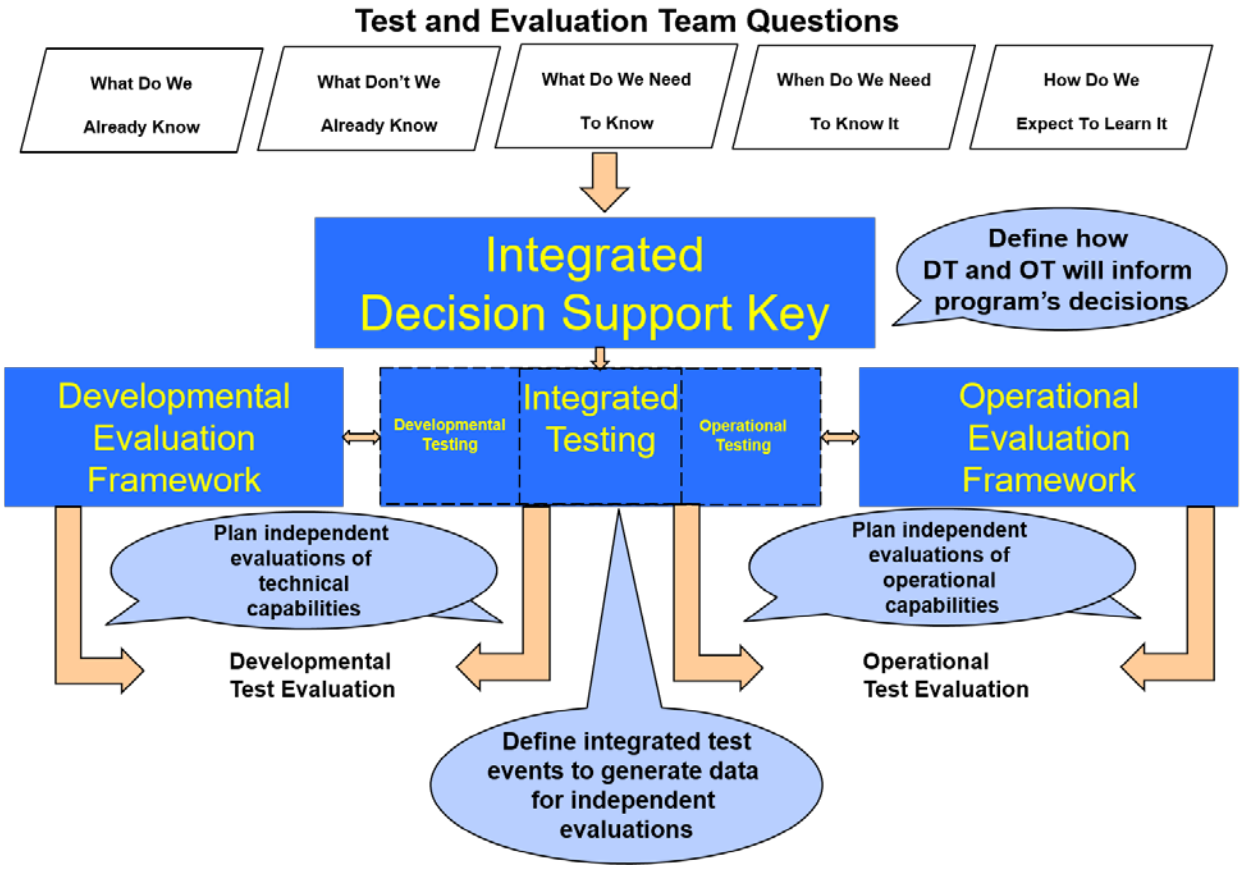
g. The T&E WIPT requires test objectives to be understood, the testing to be conducted in an operational context to the maximum extent possible, and the resultant data to be relevant for use in independent evaluations and the rationale behind the requirements. While using the T&E framework, as shown in Figure 1, it is critical that all stakeholders:

(1) Understand the scope of the evaluations required.

(2) Define, up front, the end state for evaluations.

(3) Develop an integrated testing approach that generates the data required to conduct independent evaluations.

Figure 1. Integrated T&E Framework



h. The T&E WIPT will identify DT, OT, and LFT&E data requirements needed to inform critical acquisition and engineering decisions. Once the T&E WIPT identifies the data requirements, the developmental and operational testers together will determine which data requirements can be satisfied through integrated testing and develop an integrated test matrix.

(1) All stakeholders will use the IDSK to independently develop evaluation frameworks or strategies that will show the correlation and mapping between evaluation focus areas, critical decision points, and specific data requirements.

(2) The CDT will develop the developmental evaluation framework (DEF) that focuses on the correlation between technical requirements, decision points, and data requirements.

(3) The OTA representative will develop the operational evaluation framework (OEF) that focuses on the correlation between operational issues, decision points, and data

requirements. The linkage between the OEF and the DEF shows that technical requirements support operational capabilities.

i. As part of the digital engineering strategy, models and data will be used to digitally represent the system in a mission context to conduct integrated T&E activities. To the largest extent possible, programs will use an accessible digital ecosystem (e.g., high bandwidth network, computational architectures, multi-classification environment, enterprise resources, tools, and advanced technologies). This environment must provide authoritative sources of models, data, and test artifacts (e.g., test cases, plans, deficiencies, and results) and provide digital technologies to automate, reuse, and auto-generate test artifacts to gain greater accuracy, precision, and efficiencies across integrated test resources.

j. The T&W WIPT documents the configuration of the test asset and the actual test conditions under which each element of test data was obtained. It indicates whether the test configuration represented operationally realistic or representative conditions.

k. Before the start of testing for any acquisition path, the T&E WIPT will develop and document a TEMP or similar strategic document to capture DT, OT, and LFT&E requirements; the rationale for those requirements (e.g., Joint Capabilities Integration and Development System and concept of operations (CONOPS)); and resources, to be approved by the DOT&E and USD(R&E), or their designee, as appropriate. The TEMP, or similar strategic document for programs not under T&E oversight, is approved at the Service level. At a minimum, the document details:

(1) The resources and test support requirements needed for all test phases.

(2) Developmental, operational, and live fire test objectives and test metrics.

(3) Program schedule with T&E events and reporting requirements that incorporate report generation timelines.

(4) Test phase objectives, including entrance and exit criteria and cybersecurity test objectives.

(5) Program decisions and data requirements to support those decisions.

(6) Data collection requirements.

(7) Funding sources for all test resources.

l. The PM will use the TEMP, test strategy, or other pathway-appropriate test strategy documentation as the planning and management tool for the integrated T&E program. The test strategy documentation requires DoD Component approval. Documentation for programs under USD(R&E) or DOT&E oversight will require USD(R&E), or their designee, and DOT&E approval respectively. Documentation for programs not under T&E oversight is approved at the Service level.

3.2. T&E OVERSIGHT LIST.

a. The DOT&E will manage the T&E oversight list used jointly by the USD(R&E) and DOT&E. Programs on OT and LFT&E oversight include those programs that meet the statutory definition of MDAPs in Section 2430, Title 10, U.S.C., and those that are designated by the DOT&E for oversight pursuant to Paragraph (a)(2)(B) of Section 139, Title 10, U.S.C. The DOT&E treats the latter programs as MDAPs for the purpose of OT and LFT&E oversight requirements, but not for any other purpose.

b. The DOT&E may place any program or system on the T&E oversight list at any time by using the following criteria:

(1) 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.

(2) Program has a high level of congressional or DoD interest.

(3) Weapons, equipment, or munitions that provide or enable a critical mission warfighting capability, or are a militarily significant change to a weapon system.

c. The DOT&E will provide formal notification to a Military Service when a program is being added to the T&E oversight list.

d. The DOT&E will monitor acquisition programs and consider the following to determine when programs should be removed from the T&E oversight list:

(1) T&E (initial and follow-on OT&E or LFT&E) is complete and associated reporting to inform fielding and full-rate production (FRP) decisions is complete.

(2) Program development has stabilized, and there are no significant upgrade activities.

e. The DOT&E is the approval authority for the respective 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.

f. The USD(R&E) is the approval authority for the DT&E plan in the TEMP, test strategy, or other overarching program test planning documents for all acquisition category (ACAT) ID programs. The USD(R&E) reviews and advises the MDA on the DT&E plan in the TEMP, test strategy, or other overarching program test planning documents for ACAT IB and IC programs.

g. If an Under Secretary or Service Secretary has a significant objection to a fundamental aspect of the DT&E plan, he or she may raise this objection to the Deputy Secretary of Defense in the form of a briefing. The briefing serves to notify the Deputy of a dissenting view, not to preemptively halt the relevant decision or the program office's activities. If warranted, the Deputy will intercede. Briefing requests should be made well in advance of the approval of the TEMP.

h. The T&E oversight list is unclassified. The DOT&E maintains the T&E oversight list continuously at https://osd.deps.mil/org/dote-extranet/SitePages/Home.aspx (requires login with a common access card). Classified and sensitive programs placed on T&E oversight will be identified directly to their MDAs.

i. Force protection equipment (including non-lethal weapons) will be subject to oversight, as determined by the DOT&E.

3.3. T&E MANAGEMENT.

a. As soon as practicable after the program office is established, the PM will 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.

b. PMs will designate, as soon as practicable after the program office is established, a government test agency to serve as the lead DT&E organization. For non-T&E oversight programs, a lead DT&E organization should be used, when feasible, and identified in the TEMP. The lead DT&E organization will be responsible for:

(1) Providing technical expertise on T&E concerns to the CDT.

(2) Conducting DT&E activities to support independent evaluations.

(3) Conducting DT&E activities as directed by the CDT or his or her designee.

(4) Supporting certification and accreditation activities when feasible.

(5) Assisting the CDT in providing oversight of contractors.

(6) Assisting the CDT in reaching technically informed, objective judgments about contractor and government T&E planning and results.

c. For each program, a lead OTA, lead DT organization, and lead test organization (LTO) will be designated to plan and conduct OTs, DTs, and LFT&E; report results; and provide an independent and objective evaluation of operational effectiveness, operational suitability, survivability (including cybersecurity), or lethality. They also conduct additional testing and evaluation, as required.

d. A program may use several different acquisition pathways, such as the major capability acquisition pathway that has a component or subprogram being developed through the MTA pathway and a software capability developed using the software acquisition pathway. As required in the particular pathway guidance, individual program planning documents will include a transition or integration plan that describes the T&E scope and resources following the transition.

e. T&E program documentation that already exists in other acquisition documents may be referenced as appropriate in the DOT&E- or USD(R&E)-approved T&E document. Once referenced, there is no requirement to repeat the language in the T&E program document.

f. The PM and test agencies for T&E oversight programs will provide the Defense Technical Information Center (DTIC) with all reports, and the supporting data and metadata for the test events in those reports. If there are limitations in the data or metadata that can be provided to DTIC, those limitations will be documented in the TEMP starting at MS B.

g. Test agencies will provide the DoD Modeling and Simulation Coordination Office with a descriptive summary and metadata for all accredited unclassified models or simulations that can potentially be reused by other programs.

h. The Secretaries of the Military Departments, in coordination with the DAE, the DOT&E, and the Under Secretary of Defense for Personnel and Readiness, will establish a common set of data for each major weapon system type to be collected on damage incurred during combat operations. These data will be stored in a single dedicated and accessible repository at the DTIC. The lessons learned from analyzing these data will be included, as appropriate, in both the capability requirements process and the acquisition process for new acquisitions, modifications, and upgrades.

3.4. T&E PROGRAM PLANNING.

a. The following are key considerations in developing the TEMP or other test planning documentation:

(1) The PM and the T&E WIPT will use the TEMP or other planning documentation starting at Milestone A or the decision point to enter the applicable acquisition pathway. The PM and the T&E WIPT will prepare and update the planning documentation as needed to support acquisition milestones or decision points. For FRP decision review, full deployment decision review, and thereafter, the MDA, the senior DoD Component leadership, or DOT&E (for programs on T&E oversight), may require planning documentation updates or addendums to address changes to planned or additional testing.

(2) Draft TEMPs will be available to program stakeholders as early and as frequently as possible. For oversight programs, TEMPs approved by the DoD Components will be submitted to the OSD for approval not later than 45 calendar days before the supported decision point. The PMs will ensure programs containing Information Technology (IT) are properly deconflicted with those programs' post implementation review described in DoD Instruction (DoDI) 5000.82. To support agile acquisition, the timeline for TEMP delivery may be tailored with mutual consent between the DOT&E, OTA, and program office.

(3) A TEMP may be waived or other tailored test strategy documentation be specified for certain acquisition pathways. In cases where a TEMP is not needed, early briefings to Service stakeholders (as well as the USD(R&E) and DOT&E for oversight programs) are required to facilitate cross-organizational alignment and subsequent approval of test planning documentation.

b. The TEMP or other test strategy documentation will:

(1) Contain an integrated test program summary and master schedule of all major test events or test phases to evaluate. The schedule should include the key programmatic decision points supported by the planned testing.

(a) Describe DT test events designed to evaluate performance interoperability, reliability, and cybersecurity.

(b) Describe OT test events designed to evaluate operational effectiveness, operational suitability, survivability, and cybersecurity.

(2) Include an event-driven testing schedule that will allow adequate time to support pre-test predictions; testing; post-test analysis, evaluation, and reporting; reconciliation of predictive models; and adequate time to support execution of corrective actions in response to discovered deficiencies. The schedule should allow sufficient time between DT&E and IOT&E for rework, reports, and analysis, and developmental testing of critical design changes.

(3) Be a source document for the request for proposal (RFP).

(4) Guide how contractor proposals will address program T&E needs, (e.g., test articles; T&E data rights; government access to the failure reporting; built-in test and embedded instrumentation data; government use of contractor-conducted T&E; government review and approval of contractor T&E plans; and government review of contractor evaluations).

(5) Include a DEF, live fire strategy, and an OT concept or OEF. The DEF, live fire strategy, and the OT concept identify the key data that will contribute to assessing whether the DoD is acquiring a system that supports the warfighter in accomplishing the mission.

(a) Examples of DT measures of program progress include key performance parameters (KPPs), critical technical parameters, intelligence data requirements, key system attributes, interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes, and DT objectives. In addition, the DEF will show the correlation and mapping between test events, key resources, and the decision supported.

(b) The PM and T&E WIPT should use an IDSK to ensure that the critical operational issues are not evaluating the technical specifications of the system, but are unit focused and tied to unit mission accomplishment.

(6) Identify how scientific test and analysis tools will be used to design an effective and efficient test program that will produce the required data to characterize system behavior and combat mission capability across an appropriately selected set of factors and conditions.

(7) Require all test infrastructure and tools (e.g., models, simulations, automated tools, synthetic environments) supporting acquisition decisions to be verified, validated, and accredited (VV&A) by the intended user or appropriate agency. Test infrastructure, tools, and the VV&A strategy and schedule, including the VV&A authority for each tool or test infrastructure asset,

will be documented in the TEMP, or other test strategy documentation. PMs will plan for the application and accreditation of any modeling and simulation tools supporting T&E.

(8) Require complete resource estimates for T&E to include: test articles, test sites and instrumentation, test support equipment, threat representations and simulations, intelligence mission data, test targets and expendables, support for friendly and threat operational forces used in test, models and simulations, testbeds, joint mission environment, distributed test networks, funding, manpower and personnel, training, federal/State/local requirements, range requirements, and any special requirements (e.g., explosive ordnance disposal requirements or corrosion prevention and control). Resources will be mapped against the IDSK and schedule to ensure adequacy and availability.

(9) For MDAPs, pursuant to Section 839(b) of Public Law 115-91, the PM will develop a resource table listing the initial estimates for government T&E costs in three specific categories: DT&E, OT&E, and LFT&E. This requirement also applies at each TEMP, or other test strategy documentation, update.

c. Pursuant to Section 139, Title 10, U.S.C., the DOT&E will have prompt access to all data regarding modeling and simulation activity proposed to be used by Military Departments and Defense Agencies in support of operational or LFT&E of military capabilities. This access will include data associated with VV&A activities. The PM will allow prompt access, after a test event, to the USD(R&E) and DOT&E, all records and data (including classified and propriety information, and periodic and preliminary reports of test events). Timelines for delivery for records, reports, and data will be coordinated among the stakeholders and documented in appropriate test documentation.

3.5. CYBERSECURITY T&E.

a. Cybersecurity planning and execution occurs throughout the entire life cycle. All DoD acquisition programs and systems (e.g., DBS, national security systems, weapon systems, non-developmental items), regardless of acquisition pathway, will execute the cybersecurity DT and OT iterative T&E process detailed in the DoD Cybersecurity T&E Guidebook throughout the program's life cycle, including new increments of capability. The DoD Cybersecurity T&E Guidebook provides the latest in data-driven, mission-impact-based analysis and assessment methods for cybersecurity T&E and supports assessment of cybersecurity, survivability, and resilience within a mission context and encourages planning for tighter integration with traditional system T&E.

b. The PMs will:

(1) Develop a cybersecurity strategy as part of the program protection plan based on the Joint Capabilities Integration and Development System or other system cybersecurity, survivability, and resilience requirements; known and postulated threats; derived system requirements; draft system performance specifications; and the intended operational use and environment. The cybersecurity strategy will also incorporate the appropriate aspects of the risk management framework (RMF) process (governed by DoDI 8500.01 and DoDI 8510.01) that supports obtaining an authority to operate and other items as addressed in DoD cybersecurity

policies. The cybersecurity strategy should describe how the authority to operate decision will be informed by the cybersecurity testing specified in the DoD Cybersecurity T&E Guidebook. The cybersecurity strategy should leverage integrated contractor and government testing to evaluate the security of contractor and government development capabilities of the program's sub-components, components, and integrated components; and describe the dedicated government system vulnerability and threat-based cybersecurity testing to be conducted before program product acceptance.

(2) Use the cybersecurity strategy as a source document to develop the TEMP, or other test strategy documentation. The TEMP DEF and OEF will identify specific cybersecurity data required to address the various cybersecurity stakeholder needs (PM, engineers, RMF, DT testers, OTA), crosswalk the data to develop an integrated cybersecurity T&E strategy that efficiently obtains these data, and describe how key program decisions, including the authority to operate decision, will be informed by cybersecurity testing.

(3) Determine the avenues and means by which the system and supporting infrastructure may be exploited for cyber-attack and use this information to design T&E activities and scenarios. Conduct a mission-based cyber risk assessment (such as a cyber table top) to identify those elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in T&E events.

(4) Plan to conduct contractor and government integrated tailored cooperative vulnerability identification (T&E activities to identify vulnerabilities and plan the means to mitigate or resolve them, including system scans, analysis, and architectural reviews. These activities begin with prototypes.

(5) Plan to conduct integrated tailored cybersecurity DT&E events using realistic threat exploitation techniques in representative operating environments and scenarios to exercise critical missions within a cyber-contested environment to identify any vulnerabilities and assess system cyber resilience. Whenever possible, plan threat-based testing as part of integrated contractor and government T&E.

c. The April 3, 2018 DOT&E Memorandum directs OTAs to perform a cybersecurity cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment (AA) of all acquisition programs. The January 21, 2015 DOT&E Memorandum directs OTAs to modify their cybersecurity T&E processes as appropriate for DoD systems whose functions include financial or fiscal/business activities or the management of funds. The January 21, 2015 DOT&E Memorandum also directs the OTAs to add cyber economic threat analysis, cyber economic scenario testing, and financial transaction analysis to their cybersecurity test planning for DBS.

d. The DOT&E requires testing of cybersecurity during OT&E to include the representative users and an operationally representative environment. This may include hardware; software (including embedded software and firmware); operators; maintainers; operational cyber and network defense; end users; network and system administrators; help desk; training; support documentation; tactics, techniques, and procedures; cyber threats; and other systems that input or exchange information with the system under test, as applicable.

(1) The OTAs will evaluate cybersecurity in OT&E via two assessments: a cybersecurity CVPA and an AA. The CVPA and AA should be designed to identify cyber vulnerabilities, examine attack paths, evaluate operational cyber defense capabilities, and establish the operational mission effects (e.g., loss of critical operational capability) in a cyber threat environment while conducting operational missions.

(2) The OTA, with DOT&E review and approval, should integrate developmental and operational testing where possible to ensure sufficient data are obtained to meet OT&E objectives and measures. The OTAs should review and consider data from DT events (such as the cooperative vulnerability identification and adversarial cybersecurity DT&E) and any integrated tests previously conducted. CVPA and AA results used in conjunction with the other OT&E and LFT&E results will inform the overall evaluation of operational effectiveness, suitability, and survivability.

e. All programs should plan for periodic integrated government cybersecurity test events before beginning operational testing or initial production, with the goal of increasing efficiency and effectiveness of cybersecurity T&E.

(1) Understanding that the objectives and knowledge requirements of DT&E and OT&E must be met, it is critical that the conditions of the test event and the maturity of the system under test are acceptable to both stakeholders.

(2) The system under test must be mature enough to represent the production version. The test conditions should be realistic enough to adequately represent the operational environment, while still being flexible enough to allow a wide range of penetration and adversarial activities. The goal is to maximize assessment of vulnerabilities, evaluate adversarial exploitability of those vulnerabilities, as well as evaluate recovery and restoral processes.

(3) Testing must include evaluating appropriate defensive cyberspace operations in accordance with DoDI 8530.01. The result of cybersecurity testing should be an understanding of mission critical cybersecurity vulnerabilities, each of which should then be eliminated before fielding the system.

3.6. INTEROPERABILITY T&E.

a. Interoperability testing is governed by DoDI 8330.01. All programs or acquisition paths that exchange data with an organization or site external to their Service require an interoperability certification from the Joint Interoperability Test Command, and will need to incorporate interoperability into the DT and OT.

b. IT interoperability should be evaluated early and with sufficient frequency throughout a system's life cycle to capture and assess changes affecting interoperability in a platform, joint, multinational, and interagency environment. Interoperability T&E can be tailored for the characteristics of the capability being acquired in accordance with applicable acquisition pathway policy. Interoperability certification must be granted before fielding of a new IT capability or upgrade to existing IT.

c. Working with the DoD business, warfighting, intelligence, and enterprise information environment mission area owners (Chief Management Officer of the Department of Defense, Chairman of the Joint Chiefs of Staff, Under Secretary of Defense for Intelligence and Security, and DoD Chief Information Officer) and the other DoD Component heads, the T&E WIPTs should require that capability-focused, architecture-based measures of performance and associated metrics are developed to support evaluations of IT interoperability throughout a system's life cycle and to ensure logistics assets are planned for within the T&E management plan.

3.7. NAVIGATION WARFARE (NAVWAR) COMPLIANCE T&E.

a. In accordance with the national defense strategy and DoDD 4650.05, resilient positioning, navigation, and timing (PNT) information is essential to the execution and command and control of military missions and to the efficient operation of information networks necessary for continuous situational awareness by Combatant Commanders. The DoD will employ NAVWAR capabilities to ensure a PNT advantage in support of military operations, and programs producing or using PNT information must be NAVWAR compliant. NAVWAR compliance testing is governed by DoDI 4650.08.

b. Each program or system producing or using PNT information must incorporate the system survivability KPP as defined in Paragraph 3.2.a. of DoDI 4650.08.

c. For each program or system producing or using PNT information, the PM must conduct system T&E (e.g., real-world test; modeling and simulation; empirical analysis) sufficient to validate that all systems or platforms producing or using PNT information meet the system survivability KPP referred to in Paragraph 3.7.b.

d. Pursuant to Section 1610 of Public Law 115-232, also known as "the National Defense Authorization Act for Fiscal Year 2019," the PM will systematically collect PNT T&E data, lessons learned, and design solutions. In accordance with DoDD 4650.05, the USD(R&E) and the DOT&E will share insights gained from such information with the DoD PNT Enterprise Oversight Council, as appropriate.

SECTION 4: ADAPTIVE ACQUISITION FRAMEWORK

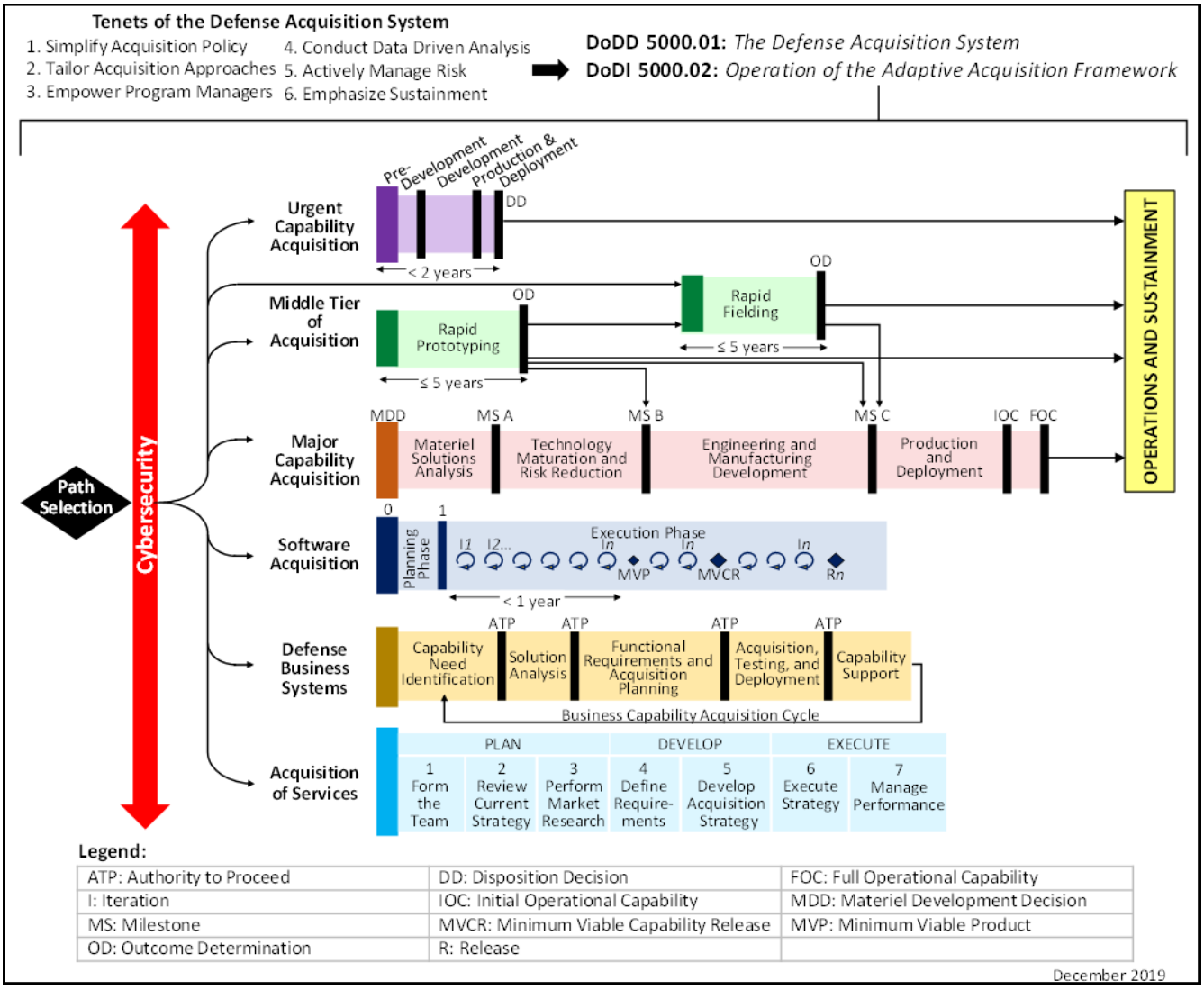
4.1. GENERAL PROCEDURES.

a. Pursuant to DoDD 5000.01 and DoDI 5000.02T, the PM will develop an acquisition strategy for MDA approval that matches the acquisition pathway (see Figure 2) processes, reviews, documents, and metrics to the character and risk of the capability being acquired.

b. Follow the overarching guidance in Paragraph 3.1 plus the pathway specific guidance in this section.

c. As applicable within each pathway, and upon coordination with the DOT&E, the DOT&E approves, in writing, the adequacy of OT&E plans for all programs on the T&E oversight list, including, but not limited to, early operational assessments (EOAs), OAs, IOT&E, and follow-on OT&E. In accordance with Section 139 of Title 10, U.S.C., OTAs provide DOT&E plans to assess adequacy of data collection and analysis planning to support the DOT&E's independent assessment of a system's operational effectiveness, operational suitability, survivability (including cybersecurity), or lethality.

Figure 2. Adaptive Acquisition Framework



4.2. T&E FOR URGENT CAPABILITY ACQUISITION PATHWAY.

a. The DOT&E will monitor all programs using the urgent capability pathway to determine placement under T&E oversight. A TEMP is not normally required. Designated programs for DOT&E operational and live fire oversight will adhere to the policies established by the DOT&E for oversight programs. These include:

(1) Approval by the DOT&E of OTPs and live fire test plans (LFTPs) at the production and development milestone. The Military Services are required to deliver test plans to the DOT&E 60 days before the start of testing.

(2) Approval by the DOT&E of post-deployment assessment plans at the production and deployment milestone.

b. Programs not under T&E oversight are approved at the Service level; the program may require a rapid and focused operational assessment (OA) and live fire testing (if applicable) before deploying an urgent need solution. The acquisition approach will identify any requirements to evaluate health, safety, or operational effectiveness, suitability, survivability, and lethality.

c. As applicable, the DOT&E will submit independent OT and live fire reports to the Secretary of Defense, the USD(A&S), congressional defense committees, and Military Services. The Secretary of Defense may authorize certain programs to defer some testing until after fielding if he or she determines the testing would unnecessarily impede the deployment of the needed capability. Testing should normally include user feedback to support design and operational use improvements and the PM's plans to correct identified deficiencies.

4.3. T&E FOR MTA PATHWAY.

a. Purpose and Applicability.

MTA programs include rapid prototyping and rapid fielding programs intended to complete in 2 to 5 years. MTA programs may be placed on the T&E oversight list and remain subject to: the LFT&E requirements in Section 2366 of Title 10, U.S.C.; IOT&E requirements in Section 2399 of Title 10, U.S.C.; LRIP quantities described in Section 2400 of Title 10, U.S.C.; and cybersecurity test requirements described in the April 3, 2018 DOT&E Memorandum. The DOT&E will determine whether to oversee an MTA program according to standards set in Paragraph 3.2.b. Memorandum.

b. General Approach for Programs on T&E Oversight.

(1) The DOT&E supports both the intent of the MTA pathway and the statutory mandate that MTA programs demonstrate and evaluate operational performance.

(2) DoDI 5000.80 requires both rapid prototyping and rapid fielding programs using the MTA pathway to develop a test strategy. Programs under T&E oversight will submit this test strategy, to include plans for operational testing and operational demonstrations (ops demos), to the DOT&E for approval. MTA ops demos offer a unique opportunity to "fly before you buy" by involving the operational user early in the acquisition process, before the initial production decision is made. The lead OTA will incorporate operational user inputs and participation in program test strategies. The DOT&E encourages tailoring MTA ops demos, and other T&E, to enable rapid fielding while maintaining acceptable risk to the warfighter.

(3) The program's decision authority will designate a DoD Component OTA to serve as the lead OTA. The PM will collaborate with the OTA and other stakeholders to develop a fully integrated test strategy. The OTA will submit plans for ops demos to the DOT&E for approval before starting the test. For programs conducting multiple ops demos, the DOT&E will tailor this approval process to ensure appropriate oversight of ops demos leading to fielding or transition to another pathway in order to minimize disrupting early testing. The DOT&E, in collaboration with the PM or OTA, will set the timeline for submitting the test strategy and OTPs

for approval. The data from all ops demos should be made available to the OTAs, the DOT&E, and other stakeholders for use to scope and inform subsequent test events and decisions.

(4) Early and continuous coordination and collaboration among the DOT&E, the PM, and the OTA will support faster reviews by the DOT&E. The PM will ensure that the OTA and DOT&E has access to ops demos and other operational, live fire, and cybersecurity test events and data. For rapid prototyping programs that will not field a significant residual operational capability to the deployed warfighter, the DOT&E will tailor the test plan approval process, which may include delegating approval authority, depending on the level of risk to the warfighter.

c. Test Strategy.

(1) To develop the test strategy, the PM may follow the streamlined TEMP guide, if that facilitates their planning, or other planning guides pre-coordinated with the OTA and DOT&E, to tailor their particular strategy to the acquisition pathway and the expected operational environment. The test strategy should present, within the context of the intended acquisition strategy, the acquisition decision that the testing will inform, program objectives and schedule including major test events and milestones, the evaluation framework, required test resources (facilities, ranges, tools, test articles, personnel, and funding), and technical or test limitations.

(2) Rapid prototyping test strategies will set evaluation criteria and milestones for technology maturity and prototype performance, culminating in an ops demo of the fieldable prototype in an operational environment. The test strategy will describe the testing that will produce the data necessary to measure technology maturity and prototype performance as well as a description of how the program will achieve a residual operational capability. Evaluation criteria should include performance, safety, interoperability, reliability, and cybersecurity. Progressive operational and live-fire assessments of capabilities and limitations, based on data from incremental integrated test events during the prototype development program, should be included in the test strategy.

(3) Rapid fielding test strategies will set evaluation criteria and milestones to demonstrate performance of the proposed products or technologies for current operational purposes. Rapid fielding decisions should be based on integrated developmental and operational testing that demonstrates how the capability contributes to fulfilling the warfighter's mission or the CONOPS. As rapid fielding programs will begin production within 6 months of program start, they typically will rely heavily on previous testing to support this accelerated timeline. The test strategy will identify all prior testing used, and will specify the additional testing necessary to address differences between the tested prototype and the planned production configuration.

d. Ops Demo.

(1) The ops demo will inform the decision whether to transition from a rapid prototyping effort, to a rapid fielding effort, to a follow-on program; or, in a rapid fielding program, to start initial production.

(2) The lead OTA will work with the CDT to develop plans for testing. In rapid prototyping, the OTA provides input to the DT plan for execution of the ops demo. For rapid

fielding, a test plan is developed. The lead OTA will plan and conduct the ops demo as an OA, with representative units, missions, and environments. Ops demos may consist of a series of incremental test events or separate "capstone" demonstration events based on program requirements. All events should be conducted in an integrated fashion, supported by collaborative developer, program office, DT, and OT planning.

(3) Ops demos should consider all aspects of system performance, including survivability and lethality if deemed critical to mission effectiveness or force protection. During the demo, operational personnel will operate the system, with the minimum necessary level of contractor support. Mission demonstrations should be designed as end-to-end missions to the maximum extent possible, to include planning, mission task execution, and post-mission activities, based on user-provided employment concepts and tactics.

(4) The OTA must submit the ops demo plan leading to a fielding decision or transition to another pathway to the DOT&E for approval before testing begins. The plan will adequately detail: 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.

e. Reporting.

(1) The OTA is responsible for producing an independent ops demo report that identifies the system's operational capabilities and limitations.

(2) The ops demo report will be delivered to the decision authority to support the initial production decision: before a rapid prototyping program transitions to a follow-on program and before a rapid fielding program begins initial production.

(3) The DOT&E will provide independent OT&E and LFT&E reports to the Office of the Secretary of Defense, Joint Staff, Military Services, and congressional defense committees as required.

4.4. T&E FOR MAJOR CAPABILITY ACQUISITION PATHWAY.

a. These acquisitions typically follow a structured analysis, design, develop, integrate, test, evaluate, produce, and support approach. This process supports MDAPs, major systems, and other complex acquisitions.

b. The USD(R&E) will prepare MS B and MS C DT&E sufficiency assessments on those MDAPs where the DAE is the MDA, in accordance with Section 838 of Public Law 115-91. For programs where the Service or the Component acquisition executive is the MDA, see Paragraph 5.3.b.(2) for additional details.

c. For programs under T&E oversight, the DOT&E will provide the MDA with milestone assessments. The DOT&E will submit a report to the Secretary of Defense and the congressional defense committees before programs under T&E oversight may proceed beyond LRIP, in accordance with Sections 2366 and 2399 of Title 10, U.S.C. Programs on T&E oversight may

not conduct operational testing until the DOT&E approves the adequacy of the plans in writing, in accordance with Section 2399(b)(1) of Title 10, U.S.C.

d. Service OTAs will conduct OT on all programs to support development, fielding decisions, and warfighter understanding of capabilities and limitations. Following initial fielding, any capability upgrades, alterations that materially change system performance, and alterations that pose substantial risk of degrading fielded military capabilities if they fail will be tested by the OTA.

e. Unless specifically waived, the test-related documentation that is required for MDAP programs will be required for all programs on DOT&E oversight, including, but not limited to, submission of Defense Intelligence Agency or DoD Component validated on-line life-cycle threat reports, test strategies, TEMPs, OTPs, LFTPs, and reporting of test results.

4.5. T&E FOR SOFTWARE ACQUISITION PATHWAY.

a. The software pathway focuses on modern iterative software development techniques such as agile, lean, and development security operations, which promise faster delivery of working code to the user. The goal of this software acquisition pathway is to achieve continuous integration and continuous delivery to the maximum extent possible. Integrated testing, to include contractor testing, is a critical component needed to reach this goal. Identifying integrated T&E and interoperability requirements early in test strategy development will enable streamlined integration, developmental and operational T&E, interoperability certification, and faster delivery to the field. The program acquisition strategy must clearly identify T&E requirements that have been fully coordinated with the test community.

b. The software pathway policy includes a requirement to create a test strategy. The program CDT or T&E lead, in collaboration with the other T&E stakeholders, should develop the test strategy and discuss the approach to developing measurable criteria derived from requirements (e.g., user features, user stories, use cases). The software pathway policy additionally requires the identification of test platforms and infrastructure be included in the acquisition strategy; the estimated T&E costs be included in the cost estimate; and the periodic delivery of the technical baseline to include scripts, tools, libraries, and other software executables necessary to test the software. Taken as whole, the test strategy for software intensive systems should include:

(1) Characterization of proposed test platforms and infrastructure, including automated testing tools and plans to accredit their use.

(2) Estimated T&E costs (DT&E, OT&E, and LFT&E).

(3) Description of the necessary contractor-developed artifacts (e.g., source code, test scripts), along with any relevant scheduling information, to support the efficient reuse in streamlining T&E.

(4) System-level performance requirements, non-functional performance requirements, and the metrics to be used to verify that the system will meet both functional and non-functional performance requirements.

(5) Key independent organizations, roles and responsibilities, and established agreements on how they will be integrated early into the developmental activities and throughout the system life cycle.

(6) How automated testing, test tools, and system telemetry will support the product throughout its life cycle.

c. The software acquisition pathway may also be applied to embedded systems. In the case of embedded software systems, the T&E strategy requires the same six features described in Paragraph 4.5.b., plus additional features, including:

(1) Approach, including resources, for testing the software in the context of the hardware with which it will eventually be integrated. This should include information on resources such as model-based environments, digital twins, and simulations, as well as plans for tests on a production-representative system.

(2) Identification of any safety critical risks, along with an approach to manage them.

d. PMs are encouraged to automate and integrate DT and OT testing to the maximum extent possible in order to accelerate acquisition timelines when feasible. This includes planning for and collecting test data from the contractor testing that can be used for evaluation. Just as the software product is being developed incrementally and iteratively in this modern software development paradigm, so too should be the T&E activities and products, particularly the test report. To maximize the benefit of early and automated data collection opportunities, the PM must collaborate with the T&E interfaces and work through the T&E processes defined for DT&E (see Section 5) and OT&E (see Section 6) to tailor a plan that will enable the effective and efficient execution of analysis and evaluation, as well as the determination of test adequacy.

(1) Automated testing should be used at the unit level, for application programming interface and integration tests, and to the maximum extent possible for user acceptance and to evaluate mission effectiveness.

(2) Automated testing tools and automated security tools should be accredited by an OTA as “fit for purpose.”

(3) Cybersecurity developmental and operational T&E assessments should consider, and reference, the DoD Cybersecurity T&E Guidebook to assist in the planning and execution of cybersecurity T&E activities needed beyond just the authority to operate (which is a necessary but not sufficient mechanism to assess cybersecurity). Automation, organic to the software acquisition pathway, provides data collection opportunities to develop cybersecurity T&E assessments in an incremental and iterative fashion.

(4) Information gleaned from automated tests, such as those detailed above, as well as other forms of tests, should be provided to the sponsor and user community for use in their periodic value assessments of the software product.

(5) The requirement for a PM to implement continuous runtime monitoring of operational software in this software acquisition pathway provides new opportunities to support operational test data requirements throughout the system life cycle.

4.6. T&E FOR THE DBS PATHWAY.

a. DBS are governed by DoDI 5000.75 and supplemented by this issuance relative to T&E.

b. DBS PMs will develop a TEMP or other test strategy documentation. The PM will describe the test strategy and essential elements of the TEMP in the DBS implementation plan. Specific T&E management content requirements in the implementation plan include:

(1) Test events to collect data must be defined, scheduled, and resourced in the implementation plan, including a DEF matrix for DT events.

(2) Cybersecurity operational T&E must also include a cyber economic vulnerability analysis as outlined in the September 14, 2010 and January 21, 2015 DOT&E Memoranda. The MDA will not tailor cybersecurity T&E solely to meet authority to operate requirements.

(3) T&E planning will include mission-oriented developmental T&E with actual operators performing end-to-end scenarios in a controlled environment to collect human-system interface data and reduce risk during operational testing.

c. Business operations testing ensures the system is working properly before the go-live decision to support OT on the live environment. Business operations testing employs actual users on the test environment performing end-to-end business transactions.

d. The CDT should plan for interoperability DT early to ensure availability of other interfacing business system test environments.

e. For programs on the T&E oversight list, the level of test and use of test data as well as dedicated OT events should be approved by the DOT&E using guidance provided in the September 14, 2010 DOT&E Memorandum. DT&E will include interoperability testing with realistic simulations or test environments of interfacing systems with operationally representative data exchanges in a controlled environment.

4.7. COMPANION GUIDE.

Additional information will be available to expand upon the T&E policy established in this issuance at the Adaptive Acquisition Framework page on the Defense Acquisition University Website at: https://www.dau.edu/aaf/

SECTION 5: DT&E

5.1. OVERVIEW.

DT&E activities support data generation for independent evaluations. They also provide program engineers and decision-makers with information to measure progress, identify problems, characterize system capabilities and limitations, and manage technical and programmatic risks. PMs use DT&E activities to manage and reduce risks during development, verify that products are compliant with contractual and technical requirements, prepare for OT, and inform decision-makers throughout the program life cycle. DT&E results verify exit criteria to ensure adequate progress before investment commitments or initiation of phases of the program, and as the basis for contract incentives.

a. DT&E starts with capability requirements and continues through product development, delivery, and acceptance; transition to OT&E; production; and operations and support. Consideration of DT&E in the requirements and systems engineering processes ensures that capability requirements are measurable, testable, and achievable. Identifying and correcting deficiencies early is less costly than discovering system deficiencies late in the acquisition process.

b. The PM will take full advantage of DoD ranges, labs, and other resources. Programs will 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, program-unique test facilities or resources.

c. Systems have become more complex, and resource constraints often force tradeoffs in the type and scope of testing that can be performed. The DT&E budget and schedule must allow testing that adequately verifies performance to contractual requirements in a controlled environment and to operational requirements.

5.2. DT&E ACTIVITIES.

a. DT&E activities will start when requirements are being developed to ensure key technical requirements are measurable, testable, and achievable; as well as provide feedback that the system engineering process is performing adequately.

b. A robust DT&E program will provide the data and assessments for independent evaluations and decision-making. The DT&E program will:

(1) Verify achievement of critical technical parameters and the ability to achieve KPPs. OT will use relevant DT data to assess progress toward achievement of critical operational issues.

(2) Assess the system's ability to achieve the thresholds prescribed in the capabilities documents.

(3) Assess system specification compliance.

(4) Provide data to the PM to enable root cause determination of failures arising from tests and to identify corrective actions.

(5) Validate system functionality in a mission context to assess readiness for OT.

(6) Provide information for cost, performance, and schedule tradeoffs.

(7) Report on the program's progress to plan for reliability growth and assess reliability and maintainability performance for use during milestone decisions.

(8) Identify system capabilities, limitations, and deficiencies.

(9) Assess system safety.

(10) Assess compatibility with legacy systems.

(11) Stress the system within the intended operationally relevant mission environment.

(12) Support all appropriate certification processes.

(13) Document achievement of contractual technical performance, and verify incremental improvements and system corrective actions.

(14) Assess entry criteria for IOT&E and follow-on OT&E.

(15) Provide DT&E data to validate parameters in models and simulations.

(16) Assess the maturity of the chosen integrated technologies.

(17) Include T&E activities to detect cyber vulnerabilities within custom and commodity hardware and software.

(18) Support cybersecurity assessments and authorization, including RMF security controls.

5.3. DT&E EXECUTION, EVALUATION, AND REPORTING.

a. DT&E Execution.

The PM and test team will develop detailed test plans for each DT event identified in the TEMP. The PM, in concert with the user and T&E community, will provide relevant safety documentation (e.g., occupational health risk acceptance) and required documentation (e.g., the National Environmental Policy Act and Executive Order 12114 documentation for the DT event, safety, and occupational health risk assessment) to testers before any test that may affect safety of personnel. The PM will conduct test readiness reviews for those events identified in the TEMP, or other test strategy documentation.

b. DT&E Evaluation.

(1) DT&E Program Assessments.

For ACAT 1B/1C programs on the T&E oversight list for which USD(R&E) did not conduct a DT&E sufficiency assessment, the USD(R&E) will provide the MDA with a program assessment at the development RFP release decision point and MS B and C. This will be updated to support the operational test readiness review or as requested by the MDA or PM. The program assessment will be based on the completed DT&E and any operational T&E activities completed to date, and will address the adequacy of the program planning, the implications of testing results to date, and the risks to successfully meeting the goals of the remaining T&E events in the program.

(2) DT&E Sufficiency Assessments.

In accordance with Sections 2366b(c)(l) and 2366c(a)(4) of Title 10, U.S.C., when the USD(A&S) is the MDA, the USD(R&E) will conduct DT&E sufficiency assessments for MDAPs to be included in MS B and MS C brief summary reports 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 will conduct DT&E sufficiency assessments for MDAPs to be included in MS B and MS C brief summary reports provided to the congressional defense committees.

c. DT&E Reports and Data.

(1) The USD(R&E) and the acquisition chain of command and their designated representatives will have full and prompt access to all ongoing developmental testing and integrated testing, and all DT and integrated test records and reports, including but not limited to: data from all tests, recurring test site status and execution reports, system logs, execution logs, test director notes, certifications, user and operator assessments, and surveys. This applies to all government-accessible data including classified, unclassified, and competition sensitive or proprietary data. Data may be preliminary and identified as such, when applicable.

(2) The PM and test agencies for all T&E oversight programs will provide DTIC with all reports and the supporting data for the test events in those reports.

(3) The DoD Components will collect and retain data from DT&E, integrated testing, and OT&E on the reliability and maintainability of ACAT I and II programs.

SECTION 6: OT&E AND LFT&E

6.1. OVERVIEW.

a. The policies described in Paragraph 4.4 of this issuance applies as overarching guidance.

b. For programs under T&E oversight, the DOT&E will provide the MDA with milestone assessments. The DOT&E will submit a report to the Secretary of Defense and the congressional defense committees before programs under T&E oversight may proceed beyond LRIP, in accordance with Sections 2366 and 2399 of Title 10, U.S.C. The report will state the opinion of the Director, as to:

(1) Whether the test and evaluation performed were adequate.

(2) Whether the results of such test and evaluation confirm that the items or components actually tested are effective and suitable for combat.

6.2. OT&E ACTIVITIES.

a. OAs.

(1) The lead OTA will prepare and report results of one or more EOAs as appropriate in support of one or more of the design phase life-cycle events (namely, the capability development document validation, the development RFP release decision point, or MS B). An EOA is typically an assessment, conducted in accordance with an approved test plan, of the program's progress in identifying operational design constraints, developing system capabilities, and reducing program risks. For programs that enter development at MS B, the lead OTA will (as appropriate) prepare and report EOA results after program initiation and before the critical design review.

(2) The lead OTA conducts an OA in accordance with a test plan approved by the DOT&E for programs that are under T&E oversight. OAs can include dedicated early operational testing, as well as developmental test results, provided they are conducted with operational realism. As a general criterion for proceeding through MS C, the lead OTA will conduct and report results of at least one OA. For an acquisition program using an incrementally deployed software program model, a risk-appropriate OA is usually required in support of every limited deployment. An OT, usually an OA, is required before deployment of accelerated or urgent acquisition programs that are under T&E or LFT&E oversight. The OTA may combine an OA with training events. An OA may not be required for programs that enter the acquisition system at MS C.

b. RFPs.

The Military Services will provide to the DOT&E and USD(R&E) an approved final draft TEMP or other test strategy documentation before release of RFPs for MS B and MS C. To the

maximum extent feasible, RFPs should be consistent with the OT program documented in the TEMP, or other test strategy documentation.

c. OT&E for Reliability and Maintainability.

The TEMP, or other test strategy documentation, will include a plan to allocate top-level reliability and maintainability requirements and rationale for the requirements that may be allocated down to the components and sub-components. Reliability allocations may include hardware and software, and may include commercial and non-developmental items.

d. Operational Test Readiness.

The DoD Components will each establish an operational test readiness review process to be executed before any OT. Before IOT&E, the process will include a review of DT&E results; an assessment of the system's progress against the KPPs, key system attributes, and critical technical parameters in the TEMP, or other test strategy documentation; an analysis of identified technical risks to verify that those risks have been retired or reduced to the extent possible during DT&E or OT&E; a review of system certifications; and a review of the IOT&E entrance criteria specified in the TEMP, or other test strategy documentation.

e. Certifications.

Testing in support of certifications should be planned in conjunction with all other testing.

(1) The PM is responsible for determining what certifications are required, involving the representatives of applicable certifying authorities in the T&E WIPT, and satisfying the certification requirements.

(2) The PM will provide the MDA, DOT&E, and the lead OTA with all data on certifications as requested.

(3) In accordance with DoDI 8330.01, all program TEMPs must reflect interoperability and supportability requirements, and serve as the basis for interoperability assessments and certifications. The preceding policies are summarized together with associated DOT&E guidance and TEMP outlines at: http://www.dote.osd.mil/temp-guidebook/index.html.

6.3. LFT&E.

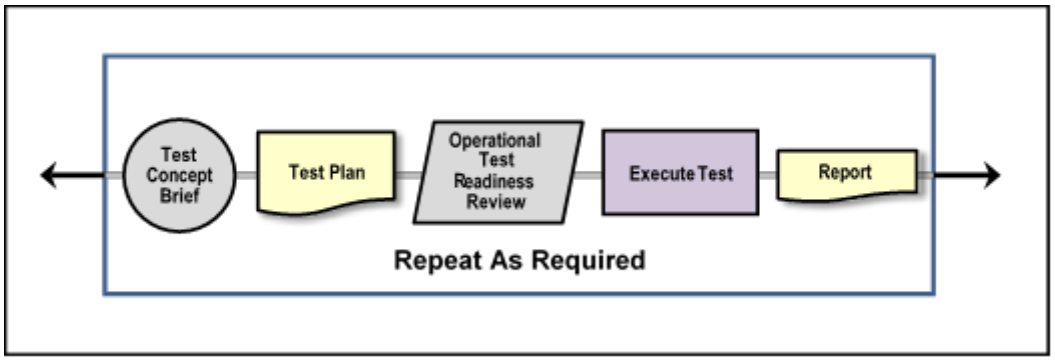
The following policy applies to all acquisition pathways as described in DoDI 5000.02T. Section 2366 of Title 10, U.S.C. mandates the LFT&E and formal LFT&E reporting for all covered systems, munition programs, missile programs, or covered product improvement programs as determined by the DOT&E. The primary emphasis is on testing vulnerability with respect to potential user casualties and taking into equal consideration the susceptibility to attack and combat performance of the system. The DOT&E will approve LFT&E strategies and LFT&E test plans (including survivability and lethality test plans) for covered systems as defined in Section 2366 of Title 10, U.S.C. LFT&E strategies and test plans may be tailored in accordance with program objectives and selected acquisition strategies. The DOT&E will

approve the quantity of test articles procured for all LFT&E test events for any system under LFT&E oversight.

6.4. OPERATIONAL AND LIVE FIRE EXECUTION.

The general process for planning, executing, and reporting on operational and live fire test events is shown in Figure 3.

Figure 3. Operational or Major Live Fire Test Event: Planning, Approval, Execution, and Reporting



a. Planning Test Events.

(1) For all programs under T&E oversight, including accelerated acquisitions, the DOT&E will approve OTPs and LFTPs before the corresponding operational or major live fire test events in accordance with Section 2399, Title 10, U.S.C. and DoDD 5141.02. The DOT&E will approve any LFTP for a major test event, such as full-up system-level test, total ship survivability trial, or full ship shock trials. The major live fire test events will be identified in the TEMP (or LFT&E strategy or equivalent document). An LTO develops test plans for both OT&E and LFT&E.

(2) For programs under T&E oversight, the appropriate LTO will brief the DOT&E on T&E concepts for the OTP or the major LFT&E as early as possible and no less than 180 calendar days before the start of any such testing. The DOT&E and DoD Component heads will be kept apprised of changes in test concept and progress on the OTP. The lead OTA will deliver the DoD Component-approved OTP for DOT&E review no later than 60 calendar days before test start. The LTO for major live fire events will deliver the DoD Component-approved LFTP for DOT&E review no later than 90 days before test start. OTPs and major LFTPs will include the plans for data collection and management. To support agile acquisition, the timetables for the test concept and OTP delivery may be tailored with mutual consent between the DOT&E, OTA, and program office; and should be negotiated via the program T&E WIPT.

(3) In OT&E, typical users or units will operate and maintain the system or item under conditions simulating combat stress in accordance with Section 139, Title 10, U.S.C., and peacetime conditions, when applicable. The lead OTA, in consultation with the user and the PM,

will identify realistic operational scenarios based on the CONOPS and mission threads derived from the joint mission essential task list or DoD Component-specific mission essential task list.

(4) Pursuant to Section 2399 of Title 10, U.S.C., persons employed by the contractor for the system being developed may only participate in OT&E of systems under T&E oversight to the extent they are planned to be involved in the operation, maintenance, and other support of the system when deployed in combat.

(5) A contractor that has participated (or is participating) in the development, production, or testing of a system for a DoD Component (or for another contractor of the DoD) may not be involved in any way in establishing criteria for data collection, performance assessment, or evaluation activities for OT&E. These limitations do not apply to a contractor that has participated in such development, production, or testing, solely in test or test support on behalf of the DoD.

(6) IOT&E for all programs will use production or production-representative test articles that, at a minimum, will incorporate the same parts and software items to be used in LRIP articles. Production-representative systems must meet the following criteria:

(a) The hardware must be as defined by the system-level critical design review, functional configuration audit, and system verification review, including correction of appropriate major deficiencies identified during prior testing. Software will be defined based on the implementation to date and the associated product roadmap.

(b) For hardware acquisitions, production-representative articles should be assembled using the parts, tools, and manufacturing processes intended for use in FRP; utilize the intended production versions of software; and the operational logistics systems including mature drafts of maintenance manuals intended for use on the fielded system should be in place. The manufacturing processes to be used in FRP should be adhered to as closely as possible, and PMs for programs under T&E oversight will provide the DOT&E a detailed description of any major manufacturing process changes.

(c) For software acquisitions, a production-representative system consists of typical users performing operational tasks with the hardware and software intended for deployment, in an operationally realistic computing environment, with representative DoD information network operations and supporting cybersecurity capabilities. All manuals, training, helpdesk, continuity of operations, system upgrades, and other life-cycle system support should be in place.

(7) IOT&E will require more than an evaluation that is based exclusively on computer modeling, simulation, or an analysis of system requirements, engineering proposals, design specifications, or any other information contained in program documents in accordance with Sections 2399 and 2366 of Title 10, U.S.C. IOT&E will feature end-to-end testing of system capabilities including all interrelated systems needed to employ and support those capabilities.

(8) PMs for all programs (and particularly accelerated acquisitions) may, in coordination with the lead OTA, elect to perform integrated testing in conjunction with training, joint and operational exercises, or synchronized test events. Such testing is efficient, but inherently increases the risk that a significant problem will not be discovered. If no subsequent operational

or live fire testing is conducted before initial fielding, then additional testing will typically be required after initial fielding. When additional testing is required, the plan for the T&E and reporting of results will be included in the applicable TEMP or other test strategy documentation.

b. Conducting Test Events.

(1) Test plans must consider the potential effects on personnel and the environment, in accordance with Sections 4321-4347 of Title 42, U.S.C., and Executive Order 12114. The T&E community, working with the PM and the user community, will provide relevant safety documentation (to include formal environment, safety, and occupational health risk acceptance for the test event) to the developmental and operational testers before any test that may affect safety of personnel.

(2) Barring significant unforeseen circumstances, all elements of an approved OTP or LFTP must be fully satisfied by the end of an operational or live fire test. If an approved plan cannot be fully executed, DOT&E concurrence with any changes must be obtained before revised test events are executed.

(a) Once testing has begun, deviations from approved elements of the test plan cannot be made without consultation with the OTA commander (for OTP), or appropriate LTO (for LFTP), and the concurrence of the DOT&E.

(b) DOT&E concurrence is not required when a need to change the execution of an element of the test plan arises in real time as its execution is underway. If DOT&E on-site representatives are not present and the test director concludes changes to the plan are warranted that would revise events yet to be conducted, the test director must contact the relevant DOT&E personnel to obtain concurrence with the proposed changes. If it is not possible to contact DOT&E personnel in a timely manner, the test director can proceed with execution of the revised test event but must inform the DOT&E of the deviations from the test plan as soon as possible.

(3) Additions to the approved test plan once the test is in execution will not occur without the concurrence of the OTA commander (for OTP), or appropriate LTO (for LFTP) and the DOT&E representative. Revisions are to be documented and signed by the test director.

(4) When the order of execution is identified in the TEMP, or other test strategy documentation, as affecting the analysis of the data, test plans should include details on the order of test event execution and test point data collection.

(5) Operating instructions (e.g., tactics, techniques, and procedures; standard operating procedures; technical manuals; technical orders) should be considered for their effect on the test outcomes and included in OTPs when relevant.

(6) Test plans must include the criteria to be used to make routine changes (e.g., delays for weather, test halts).

(7) If required data for the test completion criteria are lost, corrupted, or not gathered, then the test is not complete unless the DOT&E waives the requirement.

c. Data Management, Evaluation, and Reporting.

(1) The DOT&E, the PM, and their designated representatives who have been properly authorized access, will have full and prompt access to all records, reports, and data, including but not limited to data from tests, system logs, execution logs, test director notes, and user and operator assessments and surveys. Data include, but are not limited to, classified, unclassified, and (when available) competition sensitive or proprietary data. Data may be preliminary and will be identified as such.

(2) OTAs and other T&E agencies will record every OT&E and LFT&E event in writing. Full reports will often contain multiple test events and will be accomplished in the timeliest manner practicable. Interim summaries or catalogues of individual events will be prepared as results become available.

(3) Significant problems will be reported promptly by the acquisition decision authority to senior DoD leadership when those problems are identified. OTAs will publish interim test event summaries as interim reports when the test events provide information of immediate importance to the program decision-makers. This will occur particularly in support of accelerated acquisitions and time critical operational needs. Such reports should provide the most complete assessment possible based on the available data and should not be delayed. Such reports will be followed by the planned comprehensive reporting.

(4) For T&E and LFT&E oversight programs, the Military Services will keep the DOT&E informed of available program assets, assessments, test results, and anticipated timelines for reporting throughout report preparation.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AA	adversarial assessment
ACAT	acquisition category
CDT	chief developmental tester
CONOPS	concept of operations
CVPA	cooperative vulnerability and penetration assessment
DAE	Defense Acquisition Executive
DBS	defense business system
DEF	developmental evaluation framework
DoDD	DoD directive
DoDI	DoD instruction
DOT&E	Director of Operational Test and Evaluation
DT	developmental test
DT&E	developmental test and evaluation
DTIC	Defense Technical Information Center
EOA	early operational assessment
FRP	full-rate production
IDSK	integrated decision support key
IOT&E	initial operational test and evaluation
IT	information technology
KPP	key performance parameter
LFT&E	live fire test and evaluation
LFTP	live fire test plan
LRIP	low-rate initial production
LTO	lead test organization
MDA	milestone decision authority
MDAP	Major Defense Acquisition Program
MS B	Milestone B
MS C	Milestone C
MTA	middle tier of acquisition
NAVWAR	navigation warfare

ACRONYM	MEANING
OA	operational assessment
OEF	operational evaluation framework
ops demo	operational demonstration
OT	operational test
OT&E	operational test and evaluation
OTA	operational test agency
OTP	operational test plan
PM	program manager
PNT	positioning, navigation, and timing
RFP	request for proposal
RMF	Risk Management Framework
T&E	test and evaluation
TEMP	test and evaluation master plan
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research and Engineering
VV&A	verified, validated, and accredited
WIPT	Working-level Integrated Product Team

G.2. DEFINITIONS.

These terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
DEF	Identifies key data that will contribute to assessing system performance, interoperability, cybersecurity, reliability, and maintainability; the DEF shows the correlation and mapping between technical requirements, decision points, and data requirements.
IDSK	A table that identifies DT, OT, and LF data requirements needed to inform critical acquisition and engineering decisions (e.g., milestone decisions, key integration points, and technical readiness decisions). OT&E and DT&E will use the IDSK to independently develop evaluation frameworks or strategies that will show the correlation and mapping between evaluation focus areas, critical decision points, and specific data requirements.

TERM	DEFINITION
integrated testing	A concept that capitalizes on the idea that test events can be planned and executed to provide data for developmental, operational, and live fire evaluations.
modern software development practices	Practices (e.g., Lean, Agile, DevSecOps) that focus on rapid, iterative development and delivery of software with active user engagements. Small cross-functional software development teams integrate planning, design, development, testing, security, delivery, and operations with continuous improvement to maximize automation and user value.
OA	A test event that is conducted before initial production units are available and incorporates substantial operational realism.
OEF	Summarizes the mission-focused evaluation methodology and supporting test strategy, including the essential mission and system capabilities that contribute to operational effectiveness, operational suitability, and survivability (including cybersecurity) or lethality. It also aids integrated testing by identifying opportunities for using DT data for OT evaluation and using OT data in IT interoperability evaluation.
ops demo	An event that supports the production decisions by the decision authority.
pedigree of data	Accurately documenting the configuration of the test asset and the actual test conditions under which each element of test data were obtained. It indicates whether the test configuration represented operationally realistic or representative conditions.
TEMP	A signed agreement among the USD(R&E) or their designee, DOT&E, senior DoD Component leadership, the lead DT&E organization, the lead OTA, the MDA, and the PM.
T&E oversight list	A list of programs under DT, OT, or LFT&E oversight.

REFERENCES

Director, Operational Test and Evaluation Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," April 3, 2018

Director, Operational Test and Evaluation Memorandum, "Cyber Economic Vulnerability Assessments," January 21, 2015

Director, Operational Test and Evaluation Memorandum, "Guidelines for Operational Test and Evaluation of Information and Business Systems," September 14, 2010

DoD Cybersecurity Test and Evaluation Guidebook, April 3, 2018

DoD Directive 4650.05, "Positioning, Navigation, and Timing (PNT)," June 9, 2016, as amended

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

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

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

DoD Instruction 4650.08, "Positioning, Navigation, and Timing (PNT) and Navigation Warfare (NAVWAR)," December 27, 2018

DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015, as amended

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," February 2, 2017, as amended

DoD Instruction 5000.80, "Operation of the Middle Tier of Acquisition (MTA)," December 30, 2019

DoD Instruction 5000.82, "Acquisition of Information Technology (IT)," April 21, 2020

DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014, as amended

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

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

Executive Order 12114, "Environmental Effects Abroad of Major Federal Actions," January 4, 1979

Public Law, 91-190, "National Environmental Policy Act," January 1, 1970

Public Law, 115-91, Section 838, "National Defense Authorization Act for Fiscal Year 2018," December 12, 2017

Public Law, 115-91, Section 839(b), "National Defense Authorization Act for Fiscal Year 2018," December 12, 2017

Public Law 115-232, Section 1610, "National Defense Authorization Act for Fiscal Year 2019," August 13, 2018

United States Code, Title 10
United States Code, Title 42