BY ORDER OF THE
SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE
MANUAL 63-119

15 APRIL 2021

Acquisition

MISSION-ORIENTED TEST READINESS CERTIFICATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/TEP

Certified by: SAF/AQX
(Mr. William D. Bailey)

Supersedes: AFMAN 63-119, 26 April 2019

Pages: 103

This Department of the Air Force Manual (DAFMAN) implements Air Force Policy Directive (AFPD) 63-1/20-1, *Integrated Life Cycle Management*, and Department of the Air Force Instruction (AFI) 63-101/20-101, *Integrated Life Cycle Management.* This DAFMAN applies to system test and evaluation, and directs a process for evaluating mission-oriented test readiness certification. This continuous certification process helps keep programs on track; maximizes the likelihood of effective and suitable system performance during real world operations; and serves to document system test progress and readiness for dedicated operational test and evaluation as required by Department of Defense Instruction (DoDI) 5000.89, *Test and Evaluation*. This DAFMAN applies to civilian and uniformed members of the Regular Air Force (USAF), the United States Space Force (USSF), the Air Force Reserve, and the Air National Guard. This is a specialized publication intended for use by Airmen and Guardians who have graduated from technical training related to this publication. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*, routed through the functional chain of command. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Any organization supplementing this manual must send the proposed document to SAF Acquisition Integration (SAF/AQXS) (mail to: **SAF.AQ.SAF-**

AQXS.Workflow@us.af.mil) and AF T&E Policy, Programs, and Resources Division (AF/TEP) (mail to: **AF.TEP.Workflow@us.af.mil**) for review prior to publication. The authorities to waive requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Mandates to the acquisition execution chain as defined in AFI 63-101/20-101, including mandates to the Milestone Decision Authority (MDA), Program Executive Officer (PEO), Program Manager (PM), or other program office members, are not elevated through the organizational chain of authority; therefore tiering in accordance with DAFI 33-360, is not applied and the waiver authority is as specified. Compliance with the attachments in this publication is mandatory.

SUMMARY OF CHANGES

This document was substantially revised and needs to be completely reviewed. Major changes include the shift of focus from entrance criteria required for Operational Test (OT) to early and integrated testing and exit criteria required for mission-oriented test certification. The Department of the Air Force (DAF) has replaced the Operational Test Readiness Review (OTRR) with the Mission-Oriented Test Readiness Certification continuous evaluation process. This revision also reflects the establishment of USSF within the DAF.

Chapter 1—THE CERTIFICATION PROCESS **5**

1.1. Overview. 5

1.2. Applicability. 5

1.3. Sufficiency of Developmental Test. 6

1.4. Adequacy of Operational Test. 6

Chapter 2—ROLES AND RESPONSIBILITIES **8**

2.1. Overview of Responsibilities. 8

2.2. Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ). 8

2.3. Headquarters, U.S. Air Force, Director of Test and Evaluation (AF/TE). 8

2.4. Program Executive Officer (PEO). 8

2.5. Mission-Oriented Test Certification Official. 8

2.6. Program Managers (PMs). 8

2.7. Chief Developmental Tester (CDT), Test Manager (TM). 9

2.8. Air Force Operational Test and Evaluation Center (AFOTEC). 9

2.9. Air Force Major Command (MAJCOM) Operational Test Organization (OTO) and Space Force Command. 9

2.10. Lead Operating Command. 10
2.11. Lead Developmental Test and Evaluation Organization (LDTO). 10
2.12. Participating Test Organization(s). 10
2.13. Headquarters (HQ) DAF Staff. 10
2.14. Office of the Secretary of Defense (OSD) Staff. 10
2.15. Integrated Test Team (ITT). 10
Chapter 3—THE CERTIFICATION PROCESS 12
3.1. Overview. 12
3.2. Template Subject Matter. 12
3.3. Team Effort. 12
3.4. Tailoring the Process. 12
Figure 3.1. Matrix of Certification Templates. 13
3.5. Continuous Process. 14
3.6. The Certification Review Cycle. 16
Figure 3.2. Notional Certification Process Flowchart. 16
3.7. Certification Memo. 19
3.8. Updating the Certification Templates. 21
Chapter 4—TEMPLATE STRUCTURE AND USE 22
4.1. Interlocking Matrix. 22
4.2. Consolidation of Multiple Sources. 22
4.3. Answering Template Action Items. 22
4.4. Focus on Ends, Not Means. 22
4.5. Assigning Responsibilities. 22
4.6. Certification Template Tracking Tool. 23
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 24
Attachment 2—ACQUISITION STRATEGY & SCHEDULE 43
Attachment 3—ANALYSIS OF ALTERNATIVES (AOA) 45
Attachment 4—CAPABILITIES REQUIREMENTS DOCUMENTS (CRD) 46
Attachment 5—THREAT & INTELLIGENCE DOCUMENTS 49
Attachment 6—INTEGRATED TEST TEAM (ITT) STANDUP & ITT CHARTER 50
Attachment 7—CONCEPT OF OPERATIONS (CONOPS) 51

Attachment 8—LIFE CYCLE SUSTAINMENT PLAN (LCSP) 52

Attachment 9—INFORMATION TECHNOLOGY (IT) & NATIONAL SECURITY SYSTEMS (NSS) 54

Attachment 10—TEST & EVALUATION MASTER PLAN (TEMP) 57

Attachment 11—INTEGRATED TEST PLANNING 61

Attachment 12—CYBER RESILIENCY 63

Attachment 13—CONTRACTOR TESTING 67

Attachment 14—GOVERNMENT DEVELOPMENTAL TEST & EVALUATION (DT&E) 70

Attachment 15—SOFTWARE DEVELOPMENT & MATURITY 73

Attachment 16—LIVE FIRE TEST & EVALUATION (LFT&E) 76

Attachment 17—MODELING & SIMULATION (M&S) 78

Attachment 18—CONFIGURATION MANAGEMENT 80

Attachment 19—DEFICIENCY IDENTIFICATION & RESOLUTION PROCESSES 81

Attachment 20—PRODUCTION & OPERATIONALLY REPRESENTATIVE TEST ARTICLES 83

Attachment 21—SYSTEM PERFORMANCE 84

Attachment 22—OPERATIONAL TEST & EVALUATION (OT&E) PLAN 86

Attachment 23—INTEGRATED TECHNICAL, ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH) REVIEWS 89

Attachment 24—OPERATIONAL TEST TEAM TRAINING 92

Attachment 25—SUPPORT EQUIPMENT (SE) 93

Attachment 26—SUFFICIENCY OF SPARES 95

Attachment 27—SUPPORT AGREEMENTS 96

Attachment 28—PACKAGING, HANDLING, STORAGE & TRANSPORTATION 97

Attachment 29—PERSONNEL 98

Attachment 30—CONTRACTOR SUPPORT 99

Attachment 31—TECHNICAL DATA 101

Attachment 32—TEST & EVALUATION RESOURCES 102

Chapter 1

THE CERTIFICATION PROCESS

1.1. Overview. This DAFMAN provides a process for structured risk evaluation (cost, schedule, performance, and safety) associated with the continuum of test activity from program inception to the final stage of dedicated operational testing. The certification process is a tool to help acquisition managers and testers identify risks, reach negotiated agreements, and render accurate assessments of system readiness to achieve mission-oriented test certifications. Establishing a disciplined review and certification process in the early stages of acquisition and modification programs will culminate in more successful mission-oriented test certifications.

1.1.1. The certification process is supported by 31 certification templates in Attachments **2** through **32** based on DoD and Air Force policy, historical information, best practices, practical advice, and lessons learned from numerous acquisition programs. This continuous certification process is mandatory throughout system testing to operational acceptance, and fulfills the DoDI 5000.89, *Test and Evaluation*, and AFI 99-103, *Capabilities-Based Test and Evaluation*, OTRR requirements. **(T-0).**

1.1.2. The action items on the certification templates in Attachments **2** through **32** identify potentially applicable action items and are subordinate to DoD and/or DAF direction; e.g., directives, instructions, and manuals. The certification templates should be used together with, and not as a substitute for, formal DoD or DAF policy and guidance. For the purposes of this DAFMAN, dedicated OT refers to that phase of Operational Test and Evaluation (OT&E) that is conducted independently in support of a deployment or Full-Rate Production (FRP) decision.

1.2. Applicability. This DAFMAN supports fielding and production decisions for major acquisition programs, middle-tier acquisition programs, programs with operational demonstrations, experiments, and any other programs requiring operational testing.

1.2.1. The Mission-Oriented Test Readiness Certification process is executed for programs to evaluate system readiness for operational testing in support of deployment and/or FRP decisions. The Mission-Oriented Test Readiness Certification process includes a review of all test results (e.g., contractor, Developmental Test and Evaluation (DT&E), and OT&E), and an assessment of the system's progress. Progress is measured against the key performance parameters (KPPs), key system attributes (KSAs), and critical technical parameters documented in the test and evaluation master plan (TEMP) or other test strategy documentation. Additionally, the PM will ensure the Mission-Oriented Test Readiness Certification process includes an analysis of identified technical risks to verify those risks were managed through DT&E, a review of system certifications, and review of the OT&E entrance and exit criteria specified in the TEMP or other test strategy documentation. **(T-2).** Guidance can be found in AFI 99-103 and DoDI 5000.89.

1.2.2. Use this DAFMAN for commercial-off-the-shelf (COTS), non-developmental items (NDIs), prototypes, or any program where OT&E is planned.

1.2.3. Acquisition of non-Major Defense Acquisition Program (MDAP) defense business systems is outlined in AFMAN 63-144, *Business Capability Requirements, Compliance, And System Acquisition.* Use this DAFMAN for defense business systems that are on the Office of the Secretary of Defense (OSD) oversight list, since test planning and execution requirements

are unchanged from those specified in AFI 99-103. The OSD oversight list can be found at **https://osd.deps.mil/org/dote-extranet/SitePages/Home.aspx**.

1.2.4. Program offices using an incremental acquisition strategy in accordance with AFI 99-103 and DoDI 5000.89 will need to repeat this certification process for each increment of capability developed, produced and/or fielded. **(T-1).** For agile software development programs with planned frequent releases, the program manager should use applicable certification templates to assess OT readiness in general. The certification process described in this DAFMAN should be implemented for periodic end-to-end (especially high-volume capacity) tests of agile software development programs. For more information on agile software programs see AFI 99-103 and DoDI 5000.87, *Operation of the Software Acquisition Pathway.*

1.2.5. This DAFMAN is the primary source for the Mission-Oriented Test Readiness Certification process for all programs when the USAF or USSF is the lead service. For multi-service programs, the certification policies of the lead service are used. In these cases, this DAFMAN may or may not be the governing document as determined by the Integrated Test Team (ITT) (or equivalent body). Nonetheless, it should be used for DAF portions of certification activities. For programs where the USAF or USSF is not the lead service, USAF or USSF ITT members may adapt this process to flow into the other service's certification process.

1.2.6. Use the appropriate certification templates (found in Attachments **2** through **32**), modified as necessary, prior to deployment of prototypes, Joint Capability Technology Demonstrations, and solutions in response to Urgent Operational Needs and Joint Emergent Operational Needs to review the system's capabilities and limitations and its readiness for initial deployment. Going through the entire certification process may not be necessary in this situation but may provide insight on the sustainability of rapidly acquired capabilities. A Capabilities and Limitations Report should be provided to the developer and users. See AFI 99-103 for more information about Capabilities and Limitations Reports.

1.3. Sufficiency of Developmental Test. The MDA for MDAPs must provide an assessment of DT&E sufficiency as part of the Milestone (MS) B and MS C brief summary reports. **(T-0).** The Deputy Director for Developmental Test, Evaluation, and Assessment (DD(DTE&A)) conducts these assessments when the Under Secretary of Defense for Acquisition and Sustainment USD(A&S) is the MDA. The senior USAF or USSF DT&E official, AF/TE for both, will conduct the sufficiency assessments for MDAPs for which the Service Acquisition Executive is the MDA. **(T-0).** These DT&E assessments support the objectives of the OT certification process described in this document. The milestone (MS) B assessment must address sufficiency of DT&E plans within the TEMP, schedule, resources, mitigation of risks, and DT criteria for entering production phase. **(T-0).** For more information on acquisition milestones and MDAP definition, see DoDI 5000.85, *Major Capability Acquisition.* The MDA must ensure the MS C assessment addresses sufficiency of DT&E completed, plans and resources for remaining DT&E, mitigation of risks, and readiness of system to perform dedicated operational test and evaluation. **(T-0).** Reference DoDI 5000.89, and *Defense Acquisition Guidebook (DAG)*.

1.4. Adequacy of Operational Test. In accordance with 10 United States Code (USC) § 139, *Director of Operational Test and Evaluation*, the DOT&E reviews the adequacy of plans for operational test and evaluation. Operational Test Organizations (OTOs) will collaborate with

DOT&E action officers to determine the best approach and agree to data collection opportunities to derive test adequacy to support the various acquisition pathways and development strategies. **(T-0).** Securing adequacy is required prior to the start of the dedicated phase of OT&E; however, it is more challenging when attempting to maximize integrated testing to buy-down (or minimize) dedicated OT&E. There is no one-size-fits-all approach.

1.4.1. The best method of securing DOT&E adequacy is through DOT&E action officer early involvement, and timely and sufficient test plan documentation in the TEMP or other appropriate test strategy documentation. To maximize DOT&E adequacy approval the OTOs should document how they intend to gain maximum return (OT credit) from integrated events. As a best practice the OTOs should do the following:

1.4.1.1. Characterize the planned integrated test event and data.

1.4.1.2. Provide traceability from integrated test data to OT data needs.

1.4.1.3. Discuss what constitutes operational relevance of integrated test data (production-representative test article(s) and operationally relevant test environment)

1.4.1.4. Identify test data scoring process and/or controls for determining operational relevance.

1.4.1.5. Maintain configuration surveillance; and establish robust data collection and/or management processes and controls to mitigate contractor involvement.

1.4.2. The use of production-representative articles has traditionally been a requirement for OT adequacy. When production-representative articles are not available, the OTO may use operational-representative articles for OT adequacy if the intent is to field the capability in its current configuration regardless of plans to redesign, upgrade, or change later.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Overview of Responsibilities. The certification process cuts across organizational lines and brings together stakeholders from the acquisition, requirements, developer, information technology management, test and evaluation (T&E), operations, and sustainment communities. Other stakeholder organizations are responsible for providing test data, supporting information, studies, analyses, and candid feedback for assigned areas in support of the certification process. The following organizations or officials (or their representatives) are required to participate in the certification process.

2.2. Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ). SAF/AQ is the Air Force Service Acquisition Executive, and serves as the Milestone Decision Authority (MDA) and the Mission-Oriented Test Certification Official if the program is an MDAP, Acquisition Category (ACAT) I. SAF/AQ may delegate the Mission-Oriented Test Certification authority decision authority for the program to the PEO. SAF/AQ may appeal when OTO commanders non-concur with certification memoranda.

2.3. Headquarters, U.S. Air Force, Director of Test and Evaluation (AF/TE). Serves as the senior test executive for both the Air Force and Space Force. AF/TE may appeal when OTO commanders non-concur with certification memoranda.

2.4. Program Executive Officer (PEO). Serves as the Mission-Oriented Test Certification Official if the program is ACAT II, or on OSD oversight.

2.5. Mission-Oriented Test Certification Official. Formerly known as OT&E Certification Official, with advice from the ITT, and as designated in the TEMP or other test strategy documentation, will determine the broad scope and requirements for certifying system readiness to begin each phase of testing. **(T-2).** The Mission-Oriented Certification Official will certify test readiness. **Note:** Under no circumstance shall a PM be the Mission-Oriented Test Certification Official for their own program if the program is an MDAP, Acquisition Category (ACAT) I/II, or on the OSD oversight list. **(T-1).**

2.6. Program Managers (PMs). Will:

2.6.1. Designate a point of contact (POC) within the program office for organizing the certification process as early as possible; preferably before the first ITT meeting. **(T-3).** This POC may be the Chief Developmental Tester (CDT), Test Manager (TM), or someone else. This POC briefs the certification process and guidance found in this DAFMAN to ensure all program officials and contractors understand the overall process and how to use the applicable certification templates provided in Attachments **2** to **32**. The POC is responsible for gathering information, scheduling reviews, assigning tasks, negotiating consensus on issues and solutions, assembling certification briefings, and drafting the final certification memorandum according to this DAFMAN. **(T-3).**

2.6.2. Ensure a robust systems engineering process (e.g., Digital Engineering) serves as the underlying foundation for systems development and for reviewing and tailoring the certification templates found in Attachments **2** to **32. (T-3).** Ensure end-to-end functionality, performance, operability, and system safety during Developmental Test (DT) and prior to certification of readiness for OT. **(T-3).**

2.6.3. Ensure the capability being delivered is viable, stable, supports capability need, and furthers the acquisition strategy. **(T-3).** The capability may be, but is not limited to a component, system, subsystem, software program, application, or sprint. Test environments should be, to the extent possible, operationally relevant and realistic prior to certification. Additionally, verify that all necessary test support is available and the system has a high likelihood of a successful OT. **(T-3).** For details about system maturity levels, see *DoD Technology Readiness Assessment Guidance*.

2.6.4. Utilize the established system safety process to assure operational safety. **(T-3).** Provide required safety release prior to each testing event involving known system hazards to people, equipment, or the environment. **(T-3).**

2.6.5. Document the strategy for the certification process in Part III of the TEMP. **(T-3).**

2.6.6. Request additional stakeholder organizations to participate in this process as necessary to ensure acquisition program success. **(T-3).**

2.6.7. Ensure COTS or NDI program contracts be written such that all legacy type test data will be made available as soon as possible after contract award to permit development of the program test strategy. **(T-3).**

2.7. Chief Developmental Tester (CDT), Test Manager (TM). A designated government T&E professional in an MDAP or Major Automated Information System (MAIS) program office selected to coordinate, plan, and manage all DT&E activities, to include contractor testing, and who makes technically informed, objective judgments about DT&E results. For non-MDAP and non-MAIS programs, this person is known as the TM. The CDT (or TM) reports to the PM and co-chairs the ITT with the OTO.

2.8. Air Force Operational Test and Evaluation Center (AFOTEC). Is the Operational Test Agency (OTA) for the USAF and will act as OTA for the USSF until a USSF OTA is established. **(T-1).** If AFOTEC is designated the OTO for the program, AFOTEC will participate in the certification process as a co-chair to the ITT and will assist the PM with carrying out responsibilities as agreed. **(T-1).** They will conduct operational test utilizing the principles of test including: early involvement, tailoring test to the situation, providing continuous and cumulative feedback, streamlining their processes and products, conducting integrated and combined test, and maintaining adaptability. **(T-1).** AFOTEC will:

2.8.1. Support the PEO's certification review by presenting: current status of OT&E data collection efforts to date, any significant Mission-Based Cyber Risk Assessments (MBCRA) (e.g., Mission-based Risk Assessment Process for Cyber (MRAP-C)) and test findings identified, remaining requirements to complete the OT&E, and any risks to OT&E completion. **(T-1)**.

2.8.2. Lead the effort to mobilize resources required for dedicated OT&E; and provide advice, test support, and test data to the PM and user throughout the development process. **(T-1)**.

2.8.3. Designate a Participating Test Organization if necessary.

2.9. Air Force Major Command (MAJCOM) Operational Test Organization (OTO) and Space Force Command. If the organization is responsible for conducting OT, the MAJCOM OTO or Space Force Command will perform the same certification functions as AFOTEC would have performed. **(T-1).** OTOs will assist the PM in implementing this certification process for

operational testing when deployment and/or FRP decisions are planned. **(T-2).** OTOs can designate a Participating Test Organization. **Note:** The acronym OTO is used in the certification templates to denote either the AFOTEC OTA, MAJCOM OTO, or USSF OTO, whichever applies. See AFI 99-103 for details.

2.10. Lead Operating Command. The lead operating command, or using commands as appropriate, will participate in the certification process by assisting the PM and operational testers (e.g., AFOTEC, USAF MAJCOM OTO, or USSF OTO) and carrying out responsibilities as agreed. **(T-2).** The lead operating command provides technical and subject matter expertise to support the readiness assessment process, test resources, and will ensure operational capability requirements documents are complete and up to date according to AFI 10-601, *Operational Capability Requirements Development*, and *AF/A5R Requirements Development Guidebooks* (located on AF/A5RP's AF Portal page). **(T-2).**

2.11. Lead Developmental Test and Evaluation Organization (LDTO). Functions as the lead integrator for a program's DT&E activities. It is separate from the Program Office, but supports the PM and ITT in a provider-customer relationship with regard to scope, type and conduct of required DT&E. The LDTO assists the CDT with oversight of contractor DT&E results and managing studies, analyses and program documentation from the requirements, acquisition and cybersecurity test communities. The LDTO will plan, conduct, and report DT&E activities; and support operational and/or integrated testing of systems according to AFI 99-103 and AFI 91-202, *The US Air Force Mishap Prevention Program*. **(T-1).** The LDTO will participate in the certification process by providing sufficient analysis, results and supporting data, user comments, and recommendations to all participating PMs to support the PM's responsibilities in **paragraph 2.6**. **(T-1).** The LDTO can designate a Participating Test Organization.

2.12. Participating Test Organization(s). Will assist other test organizations in operational/integrated testing of systems according to AFI 99-103. **(T-1).** The Participating Test Organization(s) will participate in the certification process by providing sufficient analysis, results and supporting data, user comments, and recommendations to all participating PMs to support the PM's responsibilities in **paragraph 2.6**. **(T-1).**

2.13. Headquarters (HQ) DAF Staff. Representatives from SAF/AQ, SAF/A6, AF/TE and others as delegated from the above organizations, monitor the certification process for continued effectiveness and periodically update these certification templates as policy changes dictate. These staff members should attend certification proceedings when HQ DAF assistance is required.

2.14. Office of the Secretary of Defense (OSD) Staff. Staff members from the DD(DTE&A) and from the DOT&E may monitor the certification process.

2.15. Integrated Test Team (ITT). Will support the certification process by assigning key members to attend certification process reviews. **(T-1).** The CDT or TM with the lead OTO will co-chair this team and be responsible for assigning team member roles. **(T-1)**. At its discretion, the ITT may direct a sub-group (e.g., a Mission-Oriented Test Readiness Certification Group) to carry out certification responsibilities. At program inception, the ITT will build the certification process for the program's overarching strategy for T&E. **(T-1).** The ITT advises the Mission-Oriented Test Certification Official. Assigned ITT members should keep the ITT informed of issues and program status on a regular review schedule as determined by the ITT co-chairs. ITT should invite participating test organizations and other advisors to support the certification process, as appropriate (e.g., Air Force System Interoperability Test (AFSIT) and Joint Interoperability Test

Command (JITC) staff to participate for systems with net-ready performance attributes). The ITT has full authority to add or change OPRs as necessary.

Chapter 3

THE CERTIFICATION PROCESS

3.1. Overview. The certification process involves a series of systematic reviews of the applicable certification templates found in **Figure 3.1** All certification templates are found in Attachments **2** to **32.** The PM, users, developmental and operational testers, and OSD oversight representatives should coordinate regularly to address OT&E readiness and shortfalls and brief the Mission-Oriented Test Certification Official (Service Acquisition Executive, MDA, or delegated responsible PEO) who is responsible for assessing program readiness for OT&E. The certification process combines risk assessment and management techniques with a system for assigning responsibility and tracking accountability for results. Proper risk management requires systematically evaluating proposed courses of action to identify hazards and risks, eliminating them when feasible, and minimizing them when they cannot be eliminated. A proven risk management technique is to examine the successes, failures, problems, mitigation, and solutions of similar or past programs for "lessons learned" that can be applied to current programs. Another technique is to systematically comb through the entire program using specific decision criteria based on historical data. The PM has execution responsibility for T&E risk management.

3.2. Template Subject Matter. Figure 3.1 Covers a broad range of subjects to help ensure systems stay on track through DT and OT to achieve planned mission capability. Not all certification templates apply equally to every program; however, all certification templates should be considered for applicability at each review to ensure every relevant area at that point in time is covered. The initial template review should reveal where to begin working on long lead items needed much later in development programs. The certification templates are arranged in three notional groups in approximate chronological order: Test Planning and Documentation; System Design and Performance; and Test Assets and Support. The details for each subject are addressed in corresponding attachments to this manual. All certification templates are designed to increase the visibility of potential risk factors and facilitate a streamlined, executive-level review. Potential risk factors should be inclusive of all programmatic risks that will directly affect the end user such as safety, technical, operational, supportability, logistics, and any others that go beyond cost, schedule, and performance.

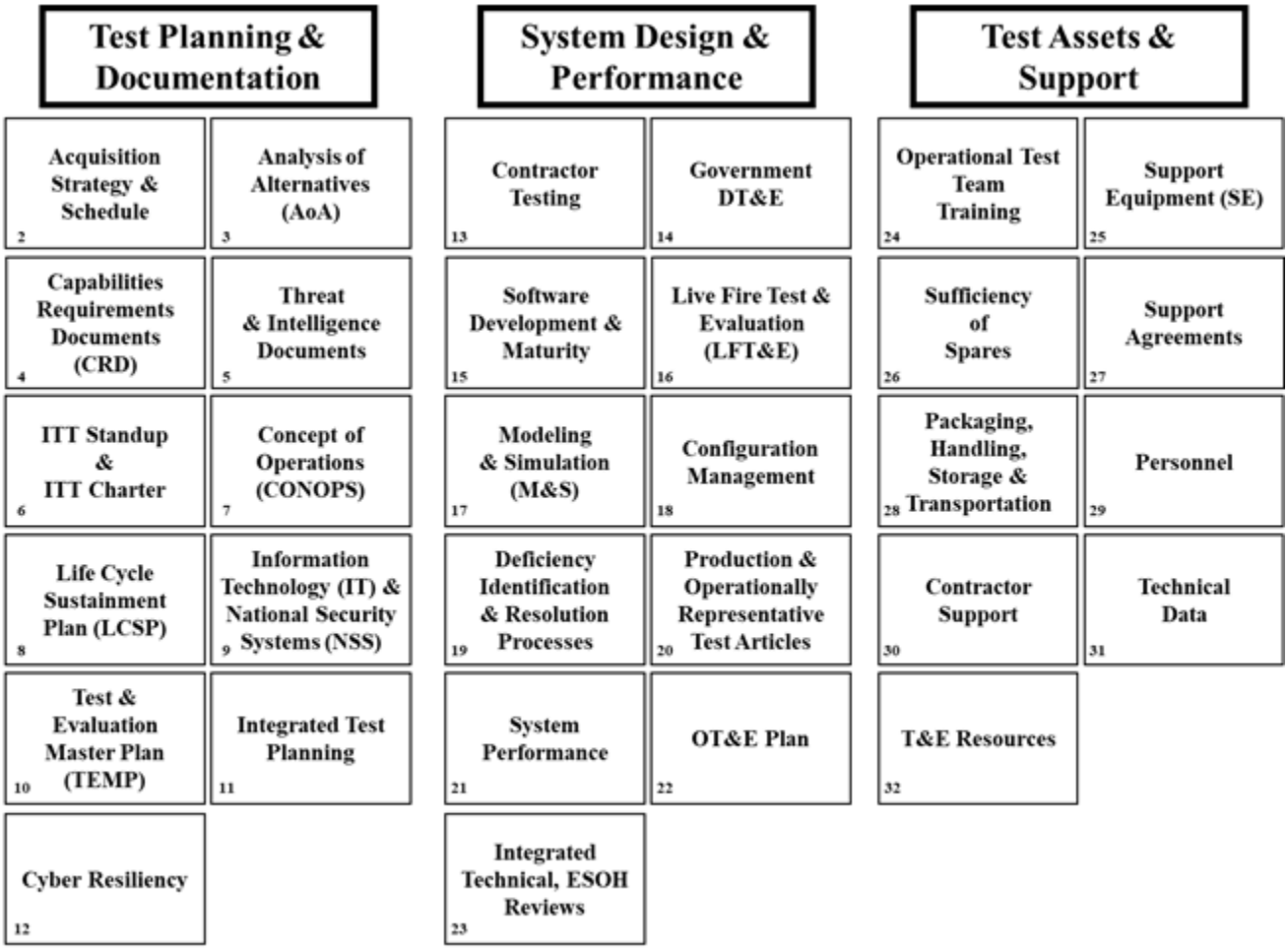
3.3. Team Effort. The risk reduction process is a team effort. Risk is managed only when conditions that contribute to risk are adequately addressed. These risk management efforts are typically within the scope, reach, and authority of certification process participants to affect necessary changes.

3.4. Tailoring the Process. As early as possible, PMs and Mission-Oriented Test Certification Officials should tailor the certification process to their need for information, program size, and complexity. The Certification Review Cycle, described in **paragraph 3.6**, should be repeated as often as necessary.

3.4.1. Use of Certification Templates. Since the certification templates are not program specific, PMs and Mission-Oriented Test Certification Officials may tailor them, with developmental tester, operational tester, and operational command assistance, to fit specific programs or groups of programs. The ITT needs to have early and continuous dialogue with the program office to accomplish the requirements addressed in the certification templates. Any deviations from an operational or production-representative article should be assessed for

potential limitations to OT&E. ITTs are encouraged to tailor the certification templates or add new ones to assist in achieving the objectives of the certification process. Some certification templates may require greater or lesser emphasis depending on the program and its phase of development. The certification templates provide PMs maximum flexibility in focusing and structuring their reviews without losing sight of the original objective—providing an executive-level review of the program. Tailoring and/or negating certification templates should only be exercised with serious consideration and should be coordinated with all stakeholders.

Figure 3.1. Matrix of Certification Templates.



Note: All acronyms in this figure are defined in **Attachment 1**.
Note: Templates are listed in approximate chronological order.

3.4.2. Tailoring Level of Detail. PMs may attach additional information or levels of detail to the certification templates at their discretion. Some examples might be exit and pass-fail criteria, action plans, requirements thresholds, lists of acquisition regulations and standards, watch lists, breakdowns of specific line items, and points of contact. Additional certification templates can be developed to cover unique areas. Additionally, aggregation of certification templates and template line items can reduce redundancy and help managers concentrate on known risk areas. In short, tailor each certification program to attain the most efficient and effective results.

3.4.3. Tailoring for Integrated Testing. Due to high levels of interdependence between types of T&E described in AFI 99-103, the scope, credibility, and success of OT&E partially depends on data provided by DT&E and other tests. Certification reviews therefore examine the types of DT&E data that are planned, and if that data can be used in support of OT&E results.

3.4.3.1. Agile Software Development involves a highly collaborative relationship between DT and OT testers, developers, and users. Integrated testing typically happens more frequently and regularly during the Agile Software Development process. Additionally, as part of leveraging development (Dev), security (Sec) and operations (Ops) (DevSecOps) principles, integrated testing may incorporate the tools and activities described in Section 4.2.4 of the *DoD Enterprise DevSecOps Reference Design*. Testers shall tailor integrated test to synchronize with developing capabilities building up to a software release. **(T-3).** Operational testers must fully engage in all software release planning in order to ensure OT&E readiness is addressed during Agile Software Development. **(T-3).**

3.4.3.2. The PM must ensure the certification incorporates adaptive test that quickly informs stakeholders and subsequent software development cycles. **(T-3).** Early OT certification involvement enables integrated testing to happen more seamlessly as a release is developed, along with decreasing administrative burden on the Program Management Office. However, separate reviews should occur and may lead to additional OT events.

3.4.4. Reporting. The resulting certification briefings and reports should be tailored to match the modified process.

3.5. Continuous Process. The Mission-Oriented test readiness certification process is viewed as a continuous effort, not a single event in time. It is not tied to any particular acquisition milestone or decision review. A certification briefing should be scheduled by the ITT to identify all completed integrated test activity, validate sufficiency of completed OT, and identify any remaining OT objectives prior to the planned start of dedicated OT as mutually agreed between the PM and operational testers.

3.5.1. Starting Early. Certification templates may be reviewed in any order that makes sense for the program and phase of development. All certification templates are initially reviewed and considered for applicability. Those that are, in the PM's judgment, clearly not relevant to the program may be set aside. Certification templates, previously set aside, could become relevant if program requirements change (e.g., when a capabilities-based requirements document is re-issued after an insertion of new technology). The PM begins the certification process as early as practical in new development programs.

3.5.2. Series of Reviews. The mission-oriented test certification process is a series of reviews designed to provide feedback to users, developers, and the test community. These reviews will also aid in resolving problems or correcting deficiencies as soon as they are discovered, rather than waiting until all DT is complete where late remedial action could cause delays in the start of any remaining OT and ultimately system delivery. **(T-1).** The PM, CDT (or TM), and OTO will determine and schedule a series of reviews based on program integrated master schedules. **(T-1)**.

3.5.3. Cyber Resiliency. A system's Cyber Resiliency involves its ability to detect an intentional (cyberattack) or unintentional cyber security incident, recover, and continue its mission. Cyber Resiliency is developed through effective application of the System Security

Engineering process to system design. It involves an intimate understanding of the threat through contextualized intelligence; development of adequate, measurable, and testable cyber requirements; and iterative cybersecurity testing, early and throughout the system's acquisition lifecycle. Intelligence support is critical to developing requirements, integrated Concept of Operations (CONOPS), and cybersecurity test measures. Early development and iterative execution of the MRAP-C methodology, a MBCRA, helps the program office understand the cyberattack surface and prioritize identified cyber risks for test, supporting the system's cyber resiliency improvement efforts.

3.5.3.1. Cyber Resiliency Testing. Cybersecurity testing highlights system cyber vulnerabilities, identifies risk to mission accomplishment, and spurs mitigation activities. From program initiation, program leadership must consider cybersecurity testing - planning, coordinating and fully integrating cybersecurity test activities into all DT and OT events (representing an operationally representative cyberspace environment). **(T-1).** The PM must plan for all aspects of cyber resiliency testing, including required resources, manpower, and infrastructure, and document in the TEMP and Capabilities Requirements Documents (CRD). **(T-3).**

3.5.3.2. Cyber Risk. A system's cyber risk may change with changes in system architecture, operating environment, and threat, necessitating additional cybersecurity testing. Early and continuous identification and resolution of cyber vulnerabilities is one of the most difficult areas for system developers, and may require more frequent review of Information Technology (IT) and National Security Systems (NSS); Cyber Resilience; and Deficiency Identification and Resolution Processes certification templates (Attachments **9**, **12**, and **19** respectively).

3.5.4. ITT Involvement. Early in the engineering and manufacturing development (EMD) phase, each program's ITT leadership should consult with their Mission-Oriented Test Certification Official to determine how to structure and tailor the certification process. The ITT should recommend the best forum and frequency for conducting the reviews.

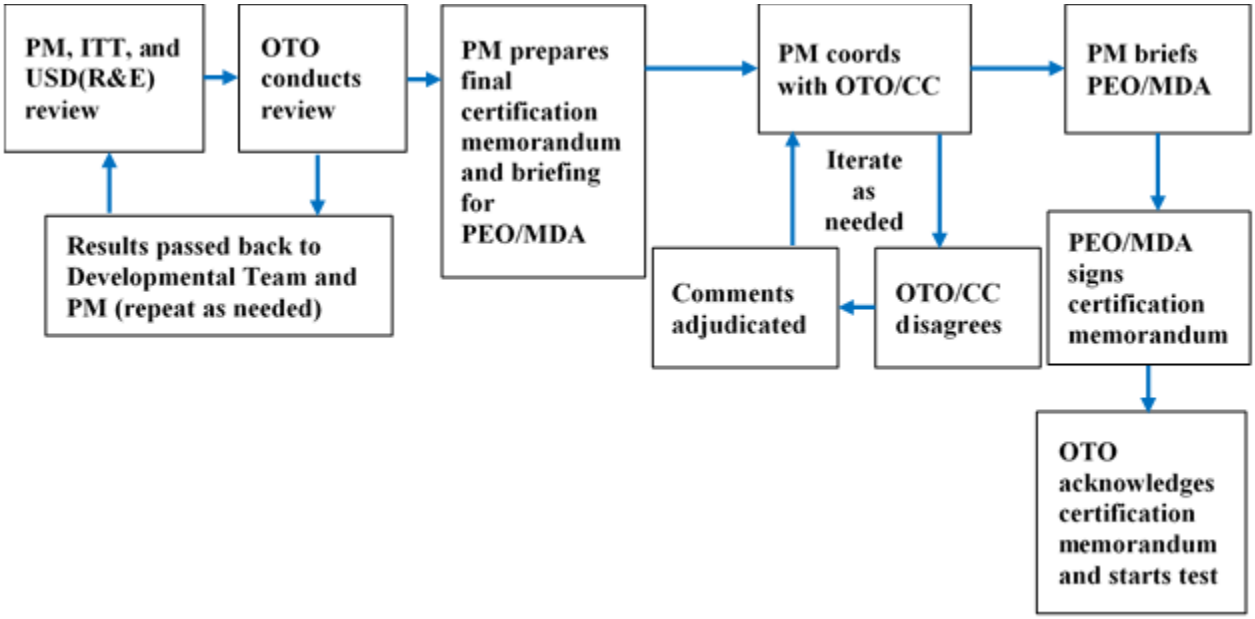
3.5.4.1. The ITT may not be the appropriate group for conducting the certification review itself due to the high-level nature of ITT membership versus the detailed nature of the material. A suggestion is to form a special Mission-Oriented Test Readiness Certification subgroup consisting of the individual stakeholders outlined in paragraphs **2.13** and **2.14**.

3.5.4.2. Frequency of Reviews. The ITT co-chairs should recommend to the Mission-Oriented Test Certification Official how to tailor the reviews to the needs of the program. In general, the frequency of reviews should increase as the program approaches the final certification date. Additional reviews may be needed for any DT&E data planned for support of OT&E. Certification reviews should be planned prior to all OT activities such as an Operational Assessment (OA).

3.5.5. Final Certification. As a minimum, a final Mission-Oriented Test Readiness Certification review and briefing should occur once all Integrated Test is complete. The ITT will schedule this event to identify all completed integrated test activity, validate sufficiency of completed OT, and identify any remaining OT objectives prior to the planned start of dedicated OT as mutually agreed between the PM and operational testers. **(T-1).** The selected date should allow the operational testers adequate time to finalize their T&E resources and schedules.

3.6. The Certification Review Cycle. A systematic series of candid review cycles, including assessments, negotiations and reporting, promotes meaningful dialogue among developers, developmental tester(s), operational tester(s), and the operating command(s). Allow sufficient staffing time for multiple cycles. The certification review OPR (CDT or TM) should periodically issue a call for roundtable meetings; create an open forum for discussion; consolidate inputs from all participating organizations and stakeholders; and report results to participants, stakeholders and the Mission-Oriented Test Certification Official. **Figure 3.2** shows the notional steps in the Certification Process and review cycle.

Figure 3.2. Notional Certification Process Flowchart.



3.6.1. Pre-Certification Reviews. A series of thorough reviews of all operational capabilities-based requirements and resource needs is the first step in assessing a program's readiness to begin OT. Each participant (e.g., subject matter expert) should review assigned areas of responsibility and intensify ongoing efforts to reach unmet goals. The purpose of multiple early reviews is to keep the PM and the Mission-Oriented Test Certification Official better informed as the program nears final certification. Thus, key issues and risks that impact OT can be identified earlier, ensuring quality, timely direction and feedback are attained from the PM and Mission-Oriented Test Certification Official.

3.6.1.1. Subject matter experts should compare demonstrated system performance to required system performance and compare available resources to required resources. A coherent, complete linkage should extend from system and/or program requirements down through the planned methods and resources for demonstrating technical and operational performance. Any flaws, inconsistencies, contradictions, voids, deficiency reports, watch items, disconnects, or cyber vulnerabilities are potential issues and areas of risk. Accurate and complete inputs are needed from all participants.

3.6.1.2. For more complex programs and systems of systems, a greater number of pre-certification reviews may be needed before the final certification review and briefing.

3.6.1.3. Under Secretary of Defense for Research and Engineering (USD(R&E)) conducts either a program assessment or DT&E Sufficiency Assessment for programs on the OSD oversight list. The PM works with DD(DTE&A) representatives to ensure this assessment supports the Mission-Oriented Test Readiness Certification. **(T-0).**

3.6.2. Assessment. Reviewers assess the shortfalls identified in the certification templates for impacts on the OT program. Candid assessment of the system's readiness to deliver the user capability needed to satisfy the operational requirements are crucial to the success of the certification process. Any shortfalls identified pose potential risk for the system not passing OT.

3.6.2.1. Standard for Assessing Readiness. Every template and template line item uses the following ideal standard for assessing system readiness and risk level: will the system be ready to deliver planned operational capability? This assessment should be based on the most current operational capabilities based requirements document, relevant military standards and specifications and the system risk assessment. Any available exit criteria should be reviewed against the relevant military standards, specifications, and requirements. The cumulative total of all judgments about these risks indicates if the system is ready for OT based on meeting the defined exit criteria. This candid assessment is the heart of the certification process.

3.6.2.2. Develop Exit Criteria. The Mission-Oriented Test Certification is a continuous process. The process includes all planned developmental and operational test activities. It also addresses incomplete testing and identified operational shortfalls. The test results, incomplete testing, and operational shortfalls are assessed to determine the system's capability to satisfy the stated operational requirements. Throughout the development process, as testing is conducted, participants should know what test events are to occur and what operational elements (if any) are to be included to simulate the intended employment and support environments to satisfy OT requirements in order to achieve the overall program goals.

3.6.2.2.1. For each identified operational shortfall, deficiency, or issue discovered during test, a specific and testable performance-based exit criterion should be developed. Satisfaction of the exit criteria in terms of demonstrated, stabilized system performance in an operationally representative environment is the best means to verify system readiness for operations, thus retesting may be required after resolution. Once all test activities both DT and OT are complete, the PEO can utilize the results to determine if the system under development satisfactorily addressed the identified operational gap and is ready for a fielding decision.

3.6.2.2.2. If all planned test activities are not complete, the PEO must make a risk-based determination of the potential impact(s) an unfavorable assessment would have on the warfighter, and develop a plan to complete any remaining testing. **(T-2).**

3.6.2.2.3. If possible, use an end-to-end integrated system test to make DT&E more operationally relevant and serve as a predictor of future operational performance. When end-to-end integrated system testing is not possible before OT, a risk assessment should support the different proposed test approaches. The program office should explain and provide plan of action to reach the exit criteria for the areas judged not ready. **(T-3).**

3.6.2.3. If Standards Are Not Met. Some template line items may not reach the ideal standard after close scrutiny. For example, technical orders (TOs) are often unavailable, produced late, or incomplete at the start of dedicated operational testing. Limitations to test may remain despite best efforts to rectify shortfalls. Several unavoidable departures from the ideal standard may occur and require constant, long-term management attention. Consider how departures from ideal standards compare to departures by previous programs and the ultimate outcomes of the OT&E campaigns of those programs. Consider both the individual departures and the number and variety of departures taken as a whole.

3.6.2.4. Action Plans. The PM must develop an action or 'get-well' plan and coordinate with the stakeholders to ensure deliberate course(s) of action are taken to reconcile any discrepancies that might prevent a smooth transition to OT&E. **(T-3).** All participants should strive to identify, track, resolve, and brief items not meeting standards as soon as they are discovered in order to optimize consensus among all participants on a solution and way forward. Every effort should be made to realistically address the associated risk level so that appropriate attention can be given at the highest levels needed to resource and best select the resolutions for the warfighter.

3.6.2.5. Deferred Requirements. If an incremental acquisition strategy is used, some operational capability requirements (and therefore the OT of those requirements) may require deferment to a later increment. These deferments may result from program cost-schedule-performance tradeoffs. Deferment of requirements (specifically, those with operational impact) must be coordinated and documented between the user and PM and eventually reflected in operational capabilities requirements documents. **(T-3).** The PM must assess the operational impacts against any deferred requirements (e.g., any dependencies, interdependencies highlighted). **(T-3).** The PM will summarize any deferred OT in the final certification briefing and memorandum. **(T-3).**

3.6.3. Negotiation. High to medium risk areas persisting after repeated reviews are likely to impact the conduct of operational testing. The PM must address risks associated with mission critical failures. **(T-3).** Certification process participants must negotiate workaround plans and solutions, or agree to some limitations on OT. **(T-3).** The program office is the focal point for attaining negotiated consensus on managing risks. Workarounds and solutions need to be in the best interests of the service. OT organization officials should be satisfied that the strength, objectivity, and independence of OT are not compromised, while the program office retains sufficient management flexibility to find optimal solutions. It is necessary to reach a corporate USAF or USSF decision on when to integrate OT.

3.6.4. Reporting. The PM, with assistance from the ITT and/or Test Community, is responsible for consolidating participants' inputs and observations and preparing the certification briefing and/or report to the Mission-Oriented Test Certification Official. Explicit action plans and exit criteria should be developed for each deficient area to bring risks to acceptable levels.

3.6.4.1. DT Report. The LDTO is responsible for providing an unbiased review of the DT results in the form of a briefing and/or report to the Mission-Oriented Test Certification Official. This may occur as part of the final certification briefing or be an independent event and/or product. It should include an independent risk assessment of the program's

ability to complete OT, if applicable, and a list or comment on any residual uncorrected potential concerns that will directly affect the warfighter.

3.6.4.2. Final Certification Briefing. The length and format of the certification briefing are discretionary and should be tailored to fit the acquisition or modification program. The order of the certification templates should not be changed. The final product should be an executive-level review of the entire program conveying enough information for senior decision-makers to make informed judgments of system readiness. The review should be tailored as a high-level, concise overview appropriate for the senior leadership's perspective, whose primary focus is to assess overall program risk along with supporting details, if required. The OTO may present their own assessment of the certification templates, especially if there is a difference of opinion as to the status of certain certification templates.

3.6.4.3. Reporting to the Mission-Oriented Test Certification Official. After reviewing the briefing or report, the PM will forward it to the Mission-Oriented Test Certification Official responsible for final mission-oriented test readiness certification. **(T-3).** The PM should brief the Mission-Oriented Test Certification Official prior to (as mutually agreed) the planned start of OT. Representatives from appropriate levels of the operating command(s), OTOs, LDTO, and other participating organizations are required to attend the briefing. **(T-1).**

3.6.4.4. Certifications for Incremental or Limited Deployment Acquisition Programs. Systems may be developed using an incremental strategy and fielded in releases of increasing capability. These systems require a final certification of readiness for each release, followed by OT for that release or limited deployment in accordance with DoDI 5000.89. The final certification for follow-on releases is briefed to the Mission-Oriented Test Certification Official and a certification memorandum submitted per certification process described in the paragraphs above.

3.6.4.5. Agile Software Development techniques release smaller capability batches that eventually build to meet a minimum viable product threshold as determined by the system requirements owner. These release cycles occur in a highly collaborative environment involving testers, users and developers that may blur the lines between DT and OT. Therefore, the handover between DT and OT is more dynamic and needs to react fast enough to keep pace with Agile Software Development velocity.

3.7. Certification Memo. The certification memorandum documents the level of agreement among certification process participants and specifies the extent of system readiness for OT within stated constraints. It confirms the certification process was properly followed. The signed certification memorandum is submitted a minimum of 15 calendar days (or as mutually agreed) before the scheduled start of OT&E. It serves as a quantifiable benchmark to check OT results against projected capabilities.

3.7.1. Tailorable. Leveraging an agile development paradigm requires highly tailored OT executed through embedded and iterative OT, and Just in Time Mission Thread Capstone (MTC) evaluations. These mission (vs. capability) tailored OT variants allow iterative risk reduction throughout the acquisition process and timely inform flow to decision makers. The certification memorandum should be tailored to certify the system is ready for the dedicated OT event. Furthermore, it should be coordinated early enough so as not to impede the

dedicated OT event, particularly if external test resources are aligned to enable the appropriate rigor prior to delivering the software release.

3.7.2. The Agile Software Development Certification Process. The OTO must be responsive to the software development velocity it is supporting while accurately portraying its current state of readiness for dedicated OT&E. **(T-3). Note:** Programs executing agile software development initiatives will need to delineate between integrated, synchronized DT and OT within iterative software development cycles versus dedicated OT events that occur at predetermined touchpoints throughout the software system's development. **(T-3).**

3.7.3. Contents. The PM must organize the certification memorandum to parallel the program's tailored certification process and discuss any agreed-upon deferments or limitations to OT. **(T-3).** The PM should not simply enumerate what was ready for OT and what was not ready, but summarize the critical areas and processes accomplished. As a minimum, the PM must address the following areas:

3.7.3.1. Briefly describe the OT; OT&E entrance and exit criteria; and which acquisition decision and increment the memorandum supports. Include anticipated operational test start and end dates (PEO is the waiver authority).

3.7.3.2. Briefly describe how the certification process was structured and executed (PEO is the waiver authority).

3.7.3.3. List the certification templates (or line items, if necessary) that are not ready or have qualifications and caveats and explain why. Describe any areas of elevated risk and how they were managed. Describe any proposed action plans, workarounds, and exit criteria, if required. **(T-1).**

3.7.3.4. List any test limitations or test deferrals, the rationale, and future plans to clear the limitations and/or deferrals. The approval of deferred items does not eliminate or alter the requirement for OT of those areas. The PM, ITT and OTO must ensure deferred items are tested in subsequent OT, or the operational requirement document is changed. **(T-1).**

3.7.3.5. List any other system attributes or mission characteristics not ready for OT&E or not expected to meet operational requirements (e.g., known deficiencies) (PEO is the waiver authority).

3.7.3.6. List any major areas of disagreement with the OTO, user(s), or other participants and accompanying rationale. **(T-1).**

3.7.4. Addressees. The PM will summarize the final certification briefing in a memorandum to the OTO commander; with information copies to SAF/AQ, AF/TE, AF/A3, AF/A4, AF/A5/8, Air Force Materiel Command (AFMC)/A3, AFMC/A2, AFMC/A5; or USSF/S2, USSF/S3, USSF/S6, USSF/S5/8; and USSF/TE, as appropriate, the capability director, the PEO, the LDTO, operational and/or using Air Force MAJCOMs or USSF Field Commands, and other participants (PEO is the waiver authority). **(T-1).** Addressee list should be tailored to program level.

3.7.5. The Mission-Oriented Test Certification Memorandum. The MDA or PEO based on the ACAT will sign the memorandum. (MDA waiver authority).

3.7.6. OTO Review. The OTO commander will acknowledge the certification memorandum before commencing OT. **(T-1).** The acknowledgment memorandum allows the OTO

commander the opportunity to concur or non-concur with the Mission-Oriented Test Certification Official's assessment, and restate any reservations or positions on unresolved issues. If agreement cannot be reached between Mission-Oriented Test Certification Official and OTO at this point, outstanding issues may be elevated to SAF/AQ and AF/TE for final resolution. The OTO commander will send an acknowledgment memorandum to the addressees, as appropriate, listed in **paragraph 3.7.4**. **(T-1).**

3.7.7. Decertification and Recertification. Despite the developer's best efforts, systems may fail to perform as planned, and continuation of OT may not be in the best interests of the government. The Mission-Oriented Test Certification Official may decertify the system and return it to DT&E based on written recommendation from the OTO or PM following a stop test due to poor system performance. The decertification memorandum includes the addressees, as appropriate, listed in **paragraph 3.7.4** Before the system resumes OT, the Mission-Oriented Test Certification Official must again certify the system via memorandum according to **paragraph 3.7** after appropriate corrective actions are taken. **(T-3).** If a system is decertified, all relevant certification templates should be revisited and the process tailored, if necessary, to improve future certification reviews of the system.

3.7.8. Alternative to Decertification. For system problems of a less serious or temporary nature, the OTO may pause testing for a brief time to assess the problem and determine if additional DT&E is warranted. **Note:** A series of pauses may indicate more serious problems requiring a stop test and system decertification.

3.8. Updating the Certification Templates. The certification process and certification templates are expected to mature through feedback from certifications and as the acquisition process continues to evolve. Further changes may result from advanced technologies, improved test and evaluation methods, revised DoD and DAF policies, and restructuring of DoD T&E processes, procedures, and practices. All users should submit AF Form 847 with their feedback on the certification process and certification templates to AF/TEP.

Chapter 4

TEMPLATE STRUCTURE AND USE

4.1. Interlocking Matrix. PMs and Mission-Oriented Test Certification Officials should utilize the certification templates to facilitate the review and help structure an executive-level briefing (MDA is the waiver authority). The certification templates (Attachments **2** through **32**) form a matrix of interlocking subject areas spanning an entire acquisition or modification program. Each template introduces order and helps reduce risk in a specific phase or aspect of a program. Some duplication and cross-referencing between certification templates are necessary because acquisition and modification programs rely on many overlapping activities. Decisions about risk in one area often affect other areas. Cross-referencing also facilitates broad area reviews as well as special subject area reviews. Closely associated certification templates are cited (e.g., See **Attachment 15**) to help find parallel information in other certification templates. **Note:** The certification templates are intended as checklists to facilitate the review and help structure the executive-level briefing. All acronyms and abbreviations are described in **Attachment 1**.

4.2. Consolidation of Multiple Sources. Each template consolidates as much practical information as possible from multiple sources into a succinct "checklist." Only a few of the most important AFIs, Chairman of the Joint Chiefs of Staff Instructions (CJCSIs), DoDIs, and Department of Defense Directives (DoDDs) are cited as footnotes to each template since complete document lists are impractical for this type and level of review, and different groups of documents may apply to different programs. Programmatic and regulatory details are left to OPRs and collateral agencies more thoroughly conversant with specialized guidance. Citation of minimum detail should help PMs, Mission-Oriented Test Certification Officials, testers, and users stay squarely focused on quality and readiness issues at the executive-level review.

4.3. Answering Template Action Items. Each template contains action items phrased as statements of fact rather than questions. Each action item should elicit a brief summary of program status in that subject area rather than a superficial "yes" or "no" response. The entire group of statements covers the template subject area, but further analysis may be required in certain cases. Action items may be answered individually or in groups depending on how the certification OPR, ITT, and/or PM tailor the certification process. Each template can function as a "tailored checklist" and as a road map for future activities in preparation for OT.

4.4. Focus on Ends, Not Means. The certification templates emphasize "what needs to be done" rather than "how to do it," leaving PMs maximum flexibility to implement their own "best practices." Full open disclosure, consistent routine reviews, and routine communication among all participants are overarching best practices.

4.5. Assigning Responsibilities. A single lead OPR is suggested for many of the line items on the certification templates to assist PMs and other participants to focus responsibility and increase accountability for results. Final determination of each OPR should be made as required to improve organizational efficiency based on who is best suited to complete each task or final product. Final approval authority for some line items may lie at higher levels. While other agencies are expected to participate on a collateral basis, multiple OPRs and offices of collateral responsibility (OCR) are not listed since responsibility would be defocused, and all variations between programs cannot be covered. Once identified and agreed upon, the OPR is expected to produce a high quality review in the assigned areas and gain the required level of participation from OCRs. The PM, with

assistance from the ITT and CDT or TM, is the OPR for ensuring the entire certification process is properly executed.

4.6. Certification Template Tracking Tool. An automated certification process tracking tool for all certification templates is available on AF/TE's AF Portal at: **https://usaf.dps.mil/:x:/r/sites/haf-te/_layouts/15/Doc.aspx?sourcedoc=%7B225016CF-EA92-41DD-83E8-57DEFDC5DC17%7D&file=AFMAN%2063-119%20Tool_20190903.xlsx&action=default&mobileredirect=true**.

Modify this tool as needed to match any changes made to the certification templates.

DARLENE J. COSTELLO
Acting Assistant Secretary of the Air Force
(Acquisition, Technology & Logistics)

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 USC § 139, *Director of Operational Test and Evaluation*

10 USC § 2366, *Major Systems and Munitions Programs: Survivability Testing and Lethality Testing Required Before Full-scale Production*

10 USC § 2399, *Operational Test and Evaluation of Defense Acquisition Programs*

10 USC § 2430, *Major Defense Acquisition Program Defined*

CJCSI 5123.01H, *Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System (JCIDS)*, 31 August 2018

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011

Joint Staff, *Cyber Survivability Endorsement Implementation Guide (CSEIG)*, V2.0, 12 March 2020

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, 22 January 2013

DoDI 3020.41, *Operational Contract Support (OCS)*, 20 December 2011

DoDI 3216.02_AFI 40-402, *Protection of Human Subjects and Adherence to Ethical Standards in Air Force Supported Research*, 10 September 2014

DoDI 4000.19, *Support Agreements*, 25 April 2013

DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*, 9 January 2009

DoDI 5000.02T, *Operation of the Defense Acquisition System*, 31 December 2020

DoDI 5000.70, *Management of DoD Modeling and Simulation (M&S) Activities*, 10 May 2012

DoDI 5000.75, *Business Systems Requirements and Acquisition*, 2 February 2017

DoDI 5000.80, *Operation of the Middle Tier of Acquisition (MTA)*, 30 December 2019

DoDI 5000.81, *Urgent Capability Acquisition*, 31 December 2019

DoDI 5000.82, *Acquisition of Information Technology (IT)*, 21 April 2020

DoDI 5000.84, *Analysis of Alternatives*, 4 August 2020

DoDI 5000.85, *Major Capability Acquisition*, 6 August 2020

DoDI 5000.86, *Acquisition Intelligence*, 11 September 2020

DoDI 5000.87, *Operation of the Software Acquisition Pathway*, 2 October 2020

DoDI 5000.89, *Test and Evaluation*, 19 November 2020

DoDI 5129.47, *Center for Countermeasures*, 26 January 2015

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),* 21 April 2016

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* 5 November 2012

DoDI 8500.01, *Cybersecurity,* 14 March 2014

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT),* 12 March 2014

DoD 5200.08-R, *Physical Security Program,* 9 April 2007

DoD 7000.14-R, *Department of Defense Financial Management Regulations,* Volume 2A, October 2008, **https://comptroller.defense.gov/FMR/fmrvolumes.aspx**

DoDM 4140.01 Volume 2, *DoD Supply Chain Materiel Management Procedures: Demand and Supply Planning,* 9 November 2018

DoDM 4140.01 Volume 7, *DoD Supply Chain Materiel Management Procedures: Supporting Technologies,* 10 February 2014

DoD CIO Memorandum, *DoD Information Enterprise Architecture,* Version 2.0, 10 July 2012

Memorandum of Agreement on Multi-Service Operational Test and Evaluation (MOT&E) and Operational Suitability Terminology and Definitions, February 2017

*Defense Acquisition Guidebook,***https://www.dau.edu/tools/dag**

DoD Cybersecurity Test and Evaluation Guidebook, Version 2.0, Change 1, 10 February 2020

DoD Enterprise DevSecOps Reference Design, Volume 1.0, 12 August 2019

DoD Guide for Achieving Reliability, Availability, and Maintainability, 3 August 2005

DoD Technology Readiness Assessment Guidance, April 2011, revised 13 May 2011

DoD Test and Evaluation Management Guide, 6th ed., December 2012, Defense Acquisition University

DoD Dictionary of Military and Associated Terms, June 2020

Incorporating Test and Evaluation into Department of Defense Acquisition Contracts, 1 October 2011

AFPD 17-1, *Information Dominance Governance and Management,* 12 April 2016

DAFI 33-360, *Publications and Forms Management,* 1 December 2015

AFI 10-601, *Operational Capability Requirements Development,* 6 November 2013

AFI 16-1001, *Verification, Validation and Accreditation (VV&A),* 29 April 2020

AFI 16-1007, *Management of Air Force Operational Training Systems,* 1 October 2019

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 6 February 2020

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures,* 18 October 2013

AFI 32-1015, *Integrated Installation Planning,* 30 July 2019

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

AFI 36-2670, *Total Force Development,* 25 June 2020

AFI 62-601, *USAF Airworthiness,* 11 June 2010

AFI 63-101/20-101, *Integrated Life Cycle Management,* 30 June 2020

AFI 63-125, *Nuclear Certification Program,* 16 January 2020

AFI 63-145, *Manufacturing and Quality Management,* 4 December 2020

AFI 65-601, *Budget Guidance and Procedures,* Volume 1, 24 October 2018

AFI 90-801, *Environment, Safety, and Occupational Health Councils,* 9 January 2020

AFI 91-202, *The US Air Force Mishap Prevention Program,* 12 March 2020

AFI 91-204, *Safety Investigation and Hazard Reporting,* 27 April 2018

AFI 91-205, *Nonnuclear Munitions Safety Board,* 23 May 2018

AFI 99-103, *Capabilities-Based Test and Evaluation,* 18 November 2019

AFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft / Data Standards,* 8 August 2019

AFMAN 32-7002, *Environmental Compliance and Pollution Prevention,* 4 February 2020

AFMAN 63-144, *Business Capability Requirements, Compliance, and System Acquisition,* 25 July 2018

AFPAM 63-113, *Program Protection Planning for Life Cycle Management,* 17 October 2013

DAFPAM 63-128, *Integrated Life Cycle Management,* 3 February 2021

AF/A5R Requirements Development Guidebook, Volumes 1-6, April 2020

Committee on National Security Systems Instruction (CNSSI) -1253, *Security Categorization and Control Selection for National Security Systems,* 27 March 2014

NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems,* February 2006

NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* 20 December 2018

NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* 23 September 2020

NIST SP 800-57, *Recommendation for Key Management,* Part 1 – General, Rev 5, 4 May 2020

NIST SP 800-57, *Recommendation for Key Management,* Part 2 – Best Practices for Key Management Organizations, Rev 1, 23 May 2019

NIST SP 800-57, *Recommendation for Key Management,* Part 3 – Application-Specific Key Management Guidance, Rev 1, 22 January 2015

MIL-STD-882, *DoD Standard Practice System Safety,* 11 May 2012

TO 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution,* 1 September 2015

TO 00-5-1, *Air Force Technical Order System,* 15 February 2019

TO 00-5-3, *Air Force Technical Order Life Cycle Management,* 15 February 2019

Prescribed Forms

None

Adopted Forms

Standard Form 368, *Product Quality Deficiency Report*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1067, *Modification Proposal*

Abbreviations and Acronyms

A&S—Acquisition and Sustainment

ACAT—Acquisition Category

AFI—Air Force Instruction

AFMC—Air Force Materiel Command

AFOTEC—Air Force Operational Test and Evaluation Center

AFPD—Air Force Policy Directive

AFSIT—Air Force System Interoperability Test

AoA—Analysis of Alternatives

ATO—Authorization to Operate or Authority to Operate

CAT—Category

CRD—Capabilities Requirements Document

CDD—Capability Development Document

CDT—Chief Developmental Tester

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CNS/ATM—Communication, Navigation, Surveillance/Air Traffic Management

CNSSI—Committee on National Security Systems (CNSS) Instruction

COI—Critical Operational Issue

CONOPS—Concept of Operations

COTS—Commercial-Off-The-Shelf

CSA—Cyber Survivability Attribute

CSEIG—Cyber Survivability Endorsement Implementation Guide

CTES—Cybersecurity test and Evaluation Strategy

CTP—Critical Technical Parameters

DAF—Department of the Air Force

DAFMAN—Department of the Air Force Manual

DAG—Defense Acquisition Guidebook

DAU—Defense Acquisition University

DD—Deputy Director

DEF—Developmental Evaluation Framework

DevSecOps—Development (Dev), Security (Sec), and Operations (Ops)

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOTMLPF—Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities

DOT&E—Director, Operational Test and Evaluation

DR—Deficiency Report/Reporting

DT—Developmental Test

DT&E—Developmental Test and Evaluation

DTE&A—Developmental Test, Evaluation, and Assessment

EMD—Engineering and Manufacturing Development

EOA—Early Operational Assessment

e.g.—for example

ESOH—Environment, Safety, and Occupational Health

FDE—Force Development Evaluation

FOT&E—Follow-on Operational Test and Evaluation

FRP—Full-Rate Production

GFE—Government Furnished Equipment

HSI—Human Systems Integration

HQ USAF—Headquarters, United States Air Force

IA—Information Assurance

ICD—Initial Capabilities Document

i.e.—that is

IMD—Intelligence Mission Data

IOT&E—Initial Operational Test and Evaluation

ISP—Information Support Plan

IT—Information Technology

ITT—Integrated Test Team

JCIDS—Joint Capabilities Integration and Development System

JIT—Just In Time

JITC—Joint Interoperability Test Command

KPP—Key Performance Parameter

KSA—Key System Attribute

LCSP—Life Cycle Sustainment Plan

LDTO—Lead Developmental Test and Evaluation Organization

LFT&E—Live Fire Test and Evaluation

LSC—Logistics Support Concepts

MAIS—Major Automated Information System

MAJCOM—Major Command

MBCRA—Mission-Based Cyber Risk Assessment

MDA—Milestone Decision Authority

MDAP—Major Defense Acquisition Program

MIL-STD—Military Standards

MRAP-C—Mission-based Risk Assessment Process for Cyber

MOA—Memorandum of Agreement

MOE—Measure of Effectiveness

MOP—Measure of Performance

MOS—Measure of Suitability

MOT&E—Multi-Service Operational Test and Evaluation

MOU—Memorandum of Understanding

MPS—Mission Planning System

MS—Milestone

MTC—Mission Thread Capstone

M&S—Modeling and Simulation

NDI—Non-Developmental Item

NIST—National Institute of Standards and Technology

NLT—not later than

NSS—National Security System

OA—Operational Assessment

OCR—Office of Collateral Responsibility

OPSEC—Operations Security

OPR—Office of Primary Responsibility

OPTEVFOR—Operational Test and Evaluation Force

OSD—Office of the Secretary of Defense

OT—Operational Test/Testing

OTA—Operational Test Agency

OTO—Operational Test Organization

OT&E—Operational Test and Evaluation

OTRR—Operational Test Readiness Review

OUE—Operational Utility Evaluation

OV—Operational View

PEO—Program Executive Officer

PIT—Platform Information Technology

PM—Program Manager

POC—Point of Contact

PPP—Program Protection Plan

QOT&E—Qualification Operational Test and Evaluation

R&E—Research and Engineering

RDT&E—Research, Development, Test and Evaluation

RMF—Risk Management Framework

SAF—Secretary of the Air Force

SAR—Safety Assessment Report

SE—Support Equipment

SEP—Systems Engineering Plan

SP—Special Publication

SS KPP—System Survivability Key Performance Parameter

STAT—Scientific Test and Analysis Techniques

SV—System View

T&E—Test and Evaluation

TBD—To Be Determined

TEMP—Test and Evaluation Master Plan

TM—Test Manager

TO—Technical Order

TRR—Test Readiness Review

USAF—United States Air Force

USC—United States Code

USD—Undersecretary of Defense

USSF—USSF

V&V—Verification and Validation

VV&A—Verification, Validation, and Accreditation

Terms

Note—See AFI 63-101/20-101 for definitions of terms relating to the requirements and acquisition processes. A common understanding of terms is essential to effectively implement this instruction. In some cases, definitions from multiple sources are offered where they may be of value. For additional terms and definitions not listed below, see *DoD Dictionary of Military and Associated Terms*. An unofficial source is the *DoD Test and Evaluation Management Guide.*

Accreditation—The official determination that a model or simulation is acceptable for use for a specific purpose. An official, written approval for the operation of a specific system in a specific environment, as documented in the certification report.

Acquisition Category (ACAT)—Acquisition categories determine the level of review, decision authority, and applicable T&E policies and procedures. They facilitate decentralized decision making and execution, and compliance with statutorily imposed requirements. See DoDI 5000.85 for details.

Airworthiness—The verified and documented capability of an air system configuration to safely attain, sustain, and terminate flight in accordance with approved usage and limits.

Authorization to Operate—The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Availability—A measure of the degree to which an item is in the operable and committable state at the start of a mission when the mission is called for at an unknown (random) time.

Blue Team—A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and

expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to verify that the customer's networks are as secure as possible before having the Red Team test the systems.

Build—The process by which source code is converted into a stand-alone form that can be run on a computer or to the form itself. **Note:** It may take several builds to reach a releasable version.

Capabilities and Limitations Report—An optional, quick-look report of limited scope that operational testers provide to operational units to support rapid and/or early fielding of developing capabilities before dedicated operational testing is complete and formal production begins. It provides the most current operational test perspectives on system capabilities and limitations based on testing done to date, and describes any untested or unknown areas.

Capabilities Requirements Document (CRD)—Any formal requirements document (e.g., Initial Capabilities Document (ICD), Capability Development Document (CDD), or DOTMLPF Change Recommendation) used to support the Joint Capabilities Integration and Development System.

Category (CAT) I—Deficiencies that may cause death, severe injury, or severe occupational illness; may cause loss or major damage to a weapon system; critically restricts the combat readiness capabilities of the using organization; or result in a production line stoppage.

Category (CAT) II—Deficiencies that impede or constrain successful mission accomplishment (impacts operational safety, suitability and effectiveness but does not meet the safety or mission impact criteria of a CAT I deficiency).

Combined Test Force—An integrated team of military, civilian, and contractor Test and Evaluation professionals empowered to plan and execute tests and report results in a collaborative, effective, and efficient manner over the entire life cycle of a system.

Common Support Equipment (SE)—Fielded SE that supports existing systems used in dedicated OT&E.

Contracting Officer—Individual with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer.

Covered System—Defined by 10 USC § 2366, *Major Systems and Munitions Programs: Survivability Testing and Lethality Testing Required Before Full-scale Production*: (1) The term "covered system" means— (A) a vehicle, weapon platform, or conventional weapon system that— (i) includes features designed to provide some degree of protection to users in combat; and (ii) is a major system as defined in section 2302(5) of this title; or (B) any other system or program designated by the Secretary of Defense for purposes of this section.

Critical Operational Issue (COI)—Operational effectiveness and operational suitability issues (not parameters, objectives, or thresholds) that are examined during operational testing to determine the system's capability to perform its mission.

Critical Technical Parameter (CTP)—Measurable critical system characteristic that, when achieved, allows the attainment of operational performance requirements. A technical measure derived from user requirements. Failure to achieve a critical technical parameter should be

considered a reliable indicator that the system is behind in the planned development schedule or will likely not achieve an operational requirement.

Cyber Resiliency—The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cyber Survivability Attribute (CSA)—Cyber Survivability verifies warfighter systems are designed to prevent, mitigate, and recover from cyber-attacks by applying a risk-managed approach to building and maintaining systems. The threat methodology employed by a cyber-review broadly accounts for mission type, cyber dependency level of the system, adversary threat tier, and impact level of system compromise in determining a cyber survivability risk category that identifies appropriate strength of implementation levels. It is accomplished through the following CSAs, as appropriate, to support the System Survivability (SS) pillars of prevent, mitigate, and recover: Prevent – CSA-01: Control Access; CSA-02: Reduce System's Cyber Detectability; CSA-03: Secure Transmissions and Communications; CSA-04: Protect System's Information from Exploitation, CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels; CSA-06: Minimize and Harden Attack Surfaces. Mitigate – CSA-07: Baseline and Monitor Systems and Detect Anomalies; CSA-08: Manage System Performance if Degraded by Cyber Events. Recover – CSA-09: System Capabilities; CSA-10: Actively Manage System's Configuration to Counter Vulnerabilities at Tactically Relevant.

Cybersecurity—Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to assure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Dedicated Operational Testing—Operational test and evaluation that is conducted independently from contractors, developers, and operating commands and used to support production or fielding decisions.

Deficiency Report (DR)—The generic term used within the USAF to record, submit, and transmit deficiency data which may include, but is not limited to, a Deficiency Report involving quality, materiel, software, warranty, or informational deficiency data submitted using SF 368, *Product Quality Deficiency Report*, or equivalent format.

Deployment—See Fielding Decision.

Developmental Test and Evaluation (DT&E)—Test and evaluation conducted to evaluate design approaches, validate analytical models, quantify contract technical performance and manufacturing quality, measure progress in system engineering design and development, minimize design risks, predict integrated system operational performance (effectiveness and suitability) in the intended environment, and identify system problems (or deficiencies) to allow for early and timely resolution. DT&E includes contractor testing and is conducted over the life of the system to support acquisition and sustainment efforts.

Early Operational Assessment (EOA)—An analysis, conducted in accordance with an approved test plan, of the program's progress in identifying operational design constraints, developing system capabilities, and mitigating program risks.

Enhancement—A condition that improves or complements successful mission accomplishment but is not absolutely required. The recommendation, if incorporated, enhances a system's

operational safety, suitability and/or effectiveness. An enhancement report should not be designated as such solely due to an "out-of-scope" condition as described in contractual requirements. Contact the Contracting Officer immediately if there is a determination that any out-of-scope requirements are contemplated for addition to the contract.

Enterprise Architecture—A well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy. Enterprise architecture applies architecture principles and practices to guide organizations through the business, information, process, and technology changes necessary to execute their strategies. These practices utilize the various aspects of an enterprise to identify, motivate, and achieve these changes

Evaluation Criteria—Standards by which the accomplishment of required technical and operational effectiveness and/or suitability characteristics, or resolution of operational issues, may be addressed.

Fault Tree Analysis—A fault tree analysis analyzes high-level failures and identifies all lower-level (sub-system) failures that cause it. Generally, the undesired event constitutes the highest level (top) event in a fault tree diagram and represents a complete or catastrophic failure of the system.

Fielding Decision—The decision to acquire and/or release a system to users in the field.

Follow-on Operational Test and Evaluations (FOT&E)—The continuation of operational test and evaluation (OT&E) after Initial Operational Test and Evaluation (IOT&E), Qualification Operational Test and Evaluation (QOT&E), or Operational Utility Evaluation (OUE) and is conducted only by AFOTEC. It answers specific questions about unresolved COIs and test issues; verifies the resolution of deficiencies or shortfalls determined to have substantial or severe impact(s) on mission operations; or completes T&E of those areas not finished during IOT&E, QOT&E, or OUE.

Force Development Evaluation (FDE)—A type of OT&E performed by OTOs in support of Air Force MAJCOM/USSF Field Command-managed system acquisition-related decisions prior to initial fielding, or for Air Force MAJCOM/USSF Field Command sustainment or upgrade activities.

Hazard—A real or potential condition that could lead to an unplanned event or series of events (e.g., mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Increment—A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed, and sustained.

Information Support Plan (ISP)—A set of information supporting interoperability test and certification. Entered through the Global Information Grid Technical Guidance Federation portal, the ISP contains or links to the Net Ready Performance Attribute along with supporting architectural data.

Initial Operational Test and Evaluation (IOT&E)—The primary dedicated OT&E of a system before FRP and/or Fielding Decision as directed by DoDI 5000.89. IOT&E determines if operational requirements and critical operational issues have been satisfied and assesses system impacts to peacetime and combat operations.

Integrated Testing—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, particularly the developmental (both contractor and government) and operational test and evaluation communities.

Integrated Test Team (ITT)—A cross-functional team of empowered representatives from multiple disciplines and organizations and co-chaired by operational testers and the program manager. The ITT is responsible for developing the strategy for T&E and the TEMP; assisting the acquisition community with T&E matters; and guiding the development of test plans that are integrated. **Note:** The ITT is the Air Force equivalent to the T&E Working-level Integrated Product Team described in DoDI 5000.89.

Interoperability—The ability of systems, units or forces to provide data, information, materiel and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle and should be balanced with information assurance.

Joint Reliability and Maintainability Evaluation Team—The team responsible for collecting, analyzing, and categorizing reliability and maintainability data during DT&E and OT&E. It is chaired by the program office during DT&E and the operational tester during dedicated operational testing. The Joint Reliability and Maintainability Evaluation Team includes representatives from the supporting and operating commands, the DT&E and OT&E test teams, and, when appropriate, system contractor personnel and nonvoting members.

Life Cycle Mission Data Plan—A statement of program needs that is applied throughout the life of an Intelligence Mission Data (IMD)-dependent acquisition program and potentially influences programmatic decisions based on the availability of IMD over the life of the program.

Life Cycle Sustainment Plan (LCSP)—A plan for the implementation, management and oversight by the designated PM of all activities associated with the acquisition, development, production, fielding, sustainment and disposal of a DoD weapon or materiel system across its life cycle.

Live Fire Test and Evaluation (LFT&E)—The firing of actual weapons (or surrogates if actual weapons are not available) at components, subsystems, sub-assemblies, and/or full-up, system-level targets or systems to examine personnel casualties, system vulnerabilities, or system lethality; and the evaluation of the results of such testing.

Logistics Support Elements—A composite of all support considerations necessary to assure the effective and economical support of a system for its life cycle. It is an integral part of all other aspects of system acquisition and operation. **Note:** The twelve logistics support elements are: Sustaining/Systems Engineering; Design Interface; Supply Support; Maintenance Planning and Management; Support Equipment/Automatic Test Systems; Facilities; Packaging, Handling, Storage, and Transportation; Technical Data Management/Technical Orders; Manpower and Personnel; Training; Computer Resources; Protection of Critical Program Information and Anti-Tamper Provisions. Formerly known as Integrated Logistics Support.

Maintainability—The capability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and routines, at each prescribed level of maintenance and repair.

Major Defense Acquisition Program (MDAP)—As defined in 10 USC § 2430, *Major Defense Acquisition Program Defined*, with the allowed adjustment amounts by Secretary of Defense under 10 USC § 2430(b), a Department of Defense acquisition program that is not a highly sensitive classified program (as determined by the Secretary of Defense) and— (A) that is designated by the Secretary of Defense as a major defense acquisition program; or (B) in the case of a program that is not a program for the acquisition of an automated information system (either a product or a service), that is estimated by the Secretary of Defense to require an eventual total expenditure for research, development, and test and evaluation of more than $525 million in Fiscal Year (FY) 2020 constant dollars or, for procurement, of more than $3.065 billion in FY 2020 constant dollars.

Measurable—Having qualitative or quantitative attributes (e.g., dimensions, velocity, capabilities) that can be ascertained and compared to known standards.

Measure of Effectiveness (MOE)—The data used to measure the military effect (mission accomplishment) that comes from the use of the system in its expected environment. That environment includes the system under test and all interrelated systems, that is, the planned or expected environment in terms of weapons, sensors, command and control, and platforms, as appropriate, needed to accomplish an end-to-end mission in combat.

Measure of Performance (MOP)—System-particular performance parameters such as speed, payload, range, time-on-station, frequency, or other distinctly quantifiable performance features. Several MOPs may be related to the achievement of a particular measure of effectiveness.

Measure of Suitability (MOS)—Measure of an item's ability to be supported in its intended operational environment. MOS's typically relate to readiness or operational availability and, hence, reliability, maintainability, and the item's support structure.

Milestone—Major decision points that separate the phases of an acquisition process.

Mission-Based Cyber Risk Assessment (MBCRA)—Process for identifying, estimating, assessing, and prioritizing risks based on impacts to DoD operational missions resulting from cyber effects on the system(s) employed.

Mission—based Risk Assessment Process for Cyber (MRAP-C)—An integrated and tailorable MBCRA process which aligns with Systems Security Engineering processes and fulfills the DoD Cybersecurity test and Evaluation Phase 1 and Phase 2 objectives. MRAP-C defines an integrated and iterative methodology to identify potential cyber risks. The MRAP-C is iteratively executed by an integrated team comprised of members from the Program Management Office, developmental, operational, and cybersecurity test agencies, and intelligence, risk management, and operational communities throughout the acquisition lifecycle to inform key decision points as the system matures. Detailed MRAP-C information is posted on the AF Portal at: **https://www.my.af.mil/gcss-af/USAF/site/MRAP-C**.

Mission-Oriented—The action of aligning to the operational purposes. Mission-oriented test readiness is the process or product that confirms the system under test will work in its intended operational environment.

Multi—Service Operational Test and Evaluation (MOT&E)—OT&E conducted by two or more service OTAs for systems acquired by more than one service. MOT&E is conducted according to the T&E directives of the lead OTO, or as agreed in a memorandum of agreement between the participants. **Note:** Air Force MAJCOM OTOs or USSF OTO may at times be responsible for conducting MOT&E in lieu of AFOTEC.

Objective Value—Value of an attribute that is applicable when a higher level of performance represents a significant increase in operational utility. The objective value is the desired operational goal achievable at a higher risk in cost, schedule, and technology. Performance above the objective does not justify the additional expense.

Operational Assessment (OA)—Incorporates substantial operational realism to assess progress toward achieving operational capabilities made by an independent operational test organization (OTO), with user support as required, on other than production systems. The focus of an operational assessment is on significant trends noted in development efforts, programmatic voids, areas of risk, adequacy of requirements, and the ability of the program to support adequate operational testing. Operational assessments may be made at any time using technology demonstrators, prototypes, mockups, engineering development models, or simulations, but are not a substitute for the dedicated OT&E necessary to support full production decisions.

Operational Effectiveness—The overall degree of mission accomplishment of a system or end item used by representative personnel in the environment planned or expected (e.g., natural, electronic, threat) for operational employment, considering organization, doctrine, tactics, cybersecurity, force protection, survivability, vulnerability, and threat (including countermeasures; initial nuclear weapons effects; and nuclear, biological, and chemical contamination threats). The PM maintains the operational effectiveness of the system by ensuring that it continues to satisfy the documented user operational capability requirements.

Operational-Representative Article—Typically based on an OTO assessment during DT or integrated testing; there are multiple definitions. 1. Any component, system, or configuration of a system, hardware or software, that provides operational capability and planned modifications to the article are deemed low-risk to the assessment results. 2. Any component, system, or configuration of a system, hardware or software, intended for fielding or operational use prior to any further modifications or upgrades (common with rapid, agile development).

Operational Safety—The level of safety risk to the system, the environment, and the occupational health caused by a system or end item when employed in an operational environment.

Operational Suitability—The degree to which a system or end item can be placed satisfactorily in field use, with consideration given to availability, compatibility, transportability, interoperability, reliability, maintainability, wartime use rates, full-dimension protection, operational safety, human factors, architectural and infrastructure compliance, manpower supportability, logistics supportability, natural environmental effects and impacts, and documentation and training requirements.

Operational Test Agency (OTA)—An independent agency reporting directly to the service Chief that plans and conducts operational tests, reports results, and provides evaluations of overall operational capability of systems as determined by effectiveness, suitability, and other operational considerations. The Air Force has the Air Force Operational Test and Evaluation Center (AFOTEC). The USSF has AFOTEC as OTA until they can establish their own USSF OTA. The

Navy has the Operational Test and Evaluation Force (OPTEVFOR). The Army has the Army Test and Evaluation Command. The Marine Corps has the Marine Corps Operational Test and Evaluation Activity.

Operational Test and Evaluation (OT&E)—Testing and evaluation conducted in as realistic an operational environment as possible to estimate the prospective system's operational effectiveness, suitability, and operational capabilities. In addition, OT&E provides information on organization, personnel requirements, doctrine, and tactics. It may also provide data to support or verify material in operating instructions, publications, and handbooks. **Note:** The generic term OT&E is often substituted for IOT&E, MOT&E, QOT&E, FOT&E, OUE, FDE, Weapons System Evaluation Program, and TD&E, and depending on the context, can have the same meaning as those terms. Refer to DoDI 5000.89 for more information on the definition of "OT&E."

Operational Testing—A generic term encompassing the entire spectrum of operationally oriented test activities, including assessments, tests, and evaluations. Not a preferred term due to its lack of specificity.

Operational Test Organization (OTO)—A generic term for any organization that conducts operational testing as stated in its mission directive.

Operational Test Readiness Review (OTRR)—A review required under DoDI 5000.89 to assess readiness for OT&E. The DAF has replaced the OTRR with the Mission-Oriented Test Readiness Certification continuous evaluation process. This process is conducted to determine changes required in planning, resources, or testing necessary to proceed with the OT&E.

Operational Utility Evaluation (OUE)—Evaluations of military capabilities conducted to demonstrate or validate new operational concepts or capabilities, upgrade components, or expand the mission or capabilities of existing or modified systems. AFOTEC, Air Force MAJCOM OTOs, or USSF OTO may conduct OUEs whenever a dedicated operational test and evaluation event is required, but the full scope and rigor of a formal IOT&E, QOT&E, FOT&E, or FDE is not appropriate or required. OUEs may be used to support operational decisions (e.g., fielding a system with less than full capability) or acquisition-related decisions (e.g., low-rate production) when appropriate throughout the system life cycle.

Oversight—Senior executive-level monitoring and review of programs to confirm compliance with policy and attainment of broad program goals.

Oversight Program—A program on the T&E oversight list for DT&E, LFT&E, and/or OT&E. The list includes all major defense acquisition programs (MDAP) (e.g., ACAT I), MAIS (e.g., ACAT IA), MDA-designated Special Interest programs and any programs selected for OSD T&E Oversight in accordance with DoDI 5000.89. The Special Interest designation is typically based on one or more of the following factors: technological complexity; congressional interest; a large commitment of resources; or the program is critical to the achievement of a capability or set of capabilities, part of a system of systems, or a joint program. Oversight programs require additional documentation and have additional review, reporting, and approval requirements.

Peculiar SE—SE under development in support of the system being tested.

Penetration Testing—A method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who have no access) and malicious insiders who have some level of authorized access.

Production-Representative Article—Any component, system or system configuration, hardware or software, which is in a form, as determined by the PM, that should not change prior to delivery and/or acceptance by the user. If the article changes after OT and before delivery and/or acceptance by the user, the OTO should evaluate the change to determine impact on OT results.

Program Manager (PM)—Applies collectively to system program directors, product group managers, single managers, acquisition program managers, and weapon system managers. Operating as the single manager, the PM has total life cycle system management authority. **Note:** This DAFMAN uses the term "PM" for any designated person in charge of acquisition activities, to include those prior to MS A (i.e., before a technology project is officially designated an acquisition program).

Prototype—A model suitable for evaluation of design, performance, and production potential. **Note:** The Air Force uses prototypes during development of a technology or acquisition program for verification or demonstration of technical feasibility. Prototypes may not be representative of the final production item.

Qualification Operational Test and Evaluation (QOT&E)—A tailored type of IOT&E performed on systems for which there is little to no Research, Development, Test and Evaluation (RDT&E)-funded development effort. COTS, NDI, and government furnished equipment (GFE) are tested in this manner.

Qualification Test and Evaluation—A tailored type of DT&E for which there is little to no RDT&E-funded development effort. COTS, NDI, and GFE are tested in this manner.

Recoverability—Following combat damage, the ability to take emergency action to prevent loss of the system, to reduce personnel casualties, or to regain weapon system combat mission capabilities.

Red Team—A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team.

Regression Testing—Type of software testing that seeks to uncover new software bugs, or regressions, in existing functional and non-functional areas of a system after changes such as enhancements, patches or configuration changes, have been made to them.

Release (pertaining to Software Development)—A delivered version of an application which may include all or part of an application.

Reliability—The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system.

Research, Development, Test and Evaluation (RDT&E) Funding—The type of funding appropriation intended for research, development, test and evaluation efforts. **Note:** The term "research and development" broadly covers the work performed by a government agency or the private sector. "Research" is the systematic study directed toward gaining scientific knowledge or understanding of a subject area. "Development" is the systematic use of the knowledge and understanding gained from research for the production of useful materials, devices, systems, or methods. RDT&E includes all supporting test and evaluation activities.

Resilience—The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Risk—A measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Defined by 1) the probability of an undesired event or condition, and 2) the consequences, impact or severity of the undesired event were it to occur.

Risk Management Framework (RMF)—Provides a disciplined and structured process that combines Information Systems security and risk management activities into the system development life cycle and authorizes their use within DoD. The RMF has six steps: categorize system; select security controls; implement security controls; assess security controls; authorize system; and monitor security controls. DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, states all DoD information technologies will be managed through RMF, consistent with the principles established in NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*,

Safety Release—The safety release is a letter provided by the PM prior to each developmental and operational test involving personnel. The safety release identifies the known Environment, Safety, and Occupational Health (ESOH) hazards that may affect the test and their associated risk acceptance. The safety release provides the T&E community the known system-related ESOH hazard data to the operators, maintainers, trainers, and testers. Test organizations use the safety release and other relevant data, documents and expertise to assess, further mitigate and accept test risks as appropriate. See AFI 91-202.

Space Flight Worthiness—The verified and documented capability of a space system configuration to safely attain, sustain, and terminate space flight in accordance with approved usage and limits.

Specification—A document intended primarily for use in procurement which clearly and accurately describes the essential technical requirements for items, materials, or services, including the procedures by which it will be determined that the requirements have been met. Specifications may be prepared to cover a group of products, services, or materials, or a single product, service, or material, and are general or detail specifications.

Strategy for T&E—A high-level conceptual outline of all T&E required to support development and sustainment of an acquisition program.

Survivability—The ability to withstand or repel attack, or other hostile action, to the extent that essential functions can continue or be resumed after onset of hostile action. (DoD 5200.08-R, *Physical Security Program*) Survivability consists of susceptibility, vulnerability, and recoverability.

Susceptibility—The inherent capacity of an asset to be affected by one or more threats or hazards. (Susceptibility is a function of operational tactics, countermeasures, probability of enemy fielding a threat, etc.) Susceptibility is considered a subset of survivability.

Sustainment—Activities that sustain systems during the operations and support phases of the system life cycle. Such activities include any investigative test and evaluation that extends the

useful military life of systems, or expands the current performance envelope or capabilities of fielded systems. Sustainment activities also include T&E for modifications and upgrade programs, and may disclose system or product deficiencies and enhancements that make further acquisitions necessary.

System—The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users.

System of Systems—A set or arrangement of related interdependent systems that provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole.

System Survivability Key Performance Parameter (SS KPP)—One of four mandatory KPPs intended to promote the development of critical warfighter capability that can survive kinetic (e.g., traditional, non-traditional, and chemical, biological, radiological and nuclear) and non-kinetic (cyber and electromagnetic spectrum (EMS)) threats across domains and applicable environment including space.

Testable—The attribute of being measurable with available test instrumentation and resources. **Note:** Testability is a broader concept indicating whether T&E infrastructure capabilities are available and capable of measuring the parameter. The difference between testable and measurable may indicate a test limitation. Some requirements may be measurable but not testable due to T&E infrastructure shortfalls, insufficient funding, safety, or statutory or regulatory prohibitions.

Test and Evaluation (T&E)—Enables 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.

Test and Evaluation Master Plan (TEMP)—Documents the overall structure and objectives of the T&E program. It provides a framework within which to generate detailed T&E plans and it documents schedule and resource implications associated with the T&E program. The TEMP identifies the necessary developmental, operational, and live-fire test activities. It relates program schedule, test management strategy and structure, and required resources to: COIs; critical technical parameters; objectives and thresholds documented in the requirements document; and milestone decision points.

Test and Evaluation Organization—Any organization whose designated mission includes test and evaluation.

Test Deferral—The movement or delay of testing and/or evaluation of a specific critical technical parameter, operational requirement, or critical operational issue to a follow-on increment or later test period. A test deferral does not change the requirement to test a system capability or function.

Test Limitation—Any condition that hampers but does not preclude adequate test and/or evaluation of a critical technical parameter, operational requirement, or critical operational issue during a T&E program.

Test Resources—A collective term that encompasses all elements necessary to plan, conduct, and collect/analyze data from a test event or program. Elements include test funding and support manpower (including temporary duty costs), test assets (or units under test), test asset support equipment, technical data, simulation models, test beds, threat simulators, surrogates and replicas, special instrumentation peculiar to a given test asset or test event, targets, tracking and data acquisition, instrumentation, equipment for data reduction, communications, meteorology, utilities, photography, calibration, security, recovery, maintenance and repair, frequency management and control, and base or facility support services.

Test Team—A group of testers and other experts who carry out integrated testing according to a specific test plan. **Note:** A combined test force is one way to organize a test team for integrated testing.

Type 1 Training—Special Contract Training. One-time or limited nature; contracted with civilian industrial or educational institutions; includes commercial off-the-shelf courses; normally used to train selected personnel to operate and maintain new systems.

Type 4 Training—Field Training. Technical training conducted at operational locations may be delivered by a field training detachment or a field training team. The field training detachment mission is to qualify personnel on new equipment and in new techniques and procedures, increase personnel skill and knowledge, acquaint personnel with specific systems, keep personnel up to date on training concepts and requirements, and maintain individuals at given proficiency levels.

Unique SE—Contractor or government furnished SE for RDT&E use only.

User—Refers to the operating command which is the primary command operating a system, subsystem, or item of equipment. Generally applies to those operating commands or organizations designated by Headquarters, US Air Force to conduct or participate in operations or operational testing, interchangeable with the term "using command." In other forums the term "warfighter" or "customer" is often used. (AFI 10-601) Also refers to maintainers. "User" is the preferred term in this DAFMAN.

Validation—Rigorous and structured process of determining the extent to which M&S accurately represents the intended "real world" phenomena from the perspective of the intended M&S use.

Verification, Validation and Accreditation (VV&A)—A continuous process in the life cycle of a model or simulation as it gets upgraded or is used for different applications.

Verification—Process of determining that M&S accurately represents the developer's conceptual description and specifications.

Vulnerability—The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment. Vulnerability is considered a subset of survivability.

Attachment 2

ACQUISITION STRATEGY & SCHEDULE

Table A2.1. Acquisition Strategy & Schedule.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Operational testers (AFOTEC or OTO) are involved early during the acquisition strategy to develop the supporting T&E strategy. (See **Attachment 10**, **Attachment 11**)
2		PM	Develop realistic, achievable, event-driven acquisition and test schedules and check they are harmonized throughout all program documents. Avoid success-dependent schedules.
3		PM	Congressional and Planning, Programming, Budgeting, and Execution schedule constraints are incorporated into the acquisition schedule.
4		PM	Sufficient and timely RDT&E funding and procurement appropriations are programmed during each budget cycle to keep the program in technical balance.
5		PM	Schedule sufficient numbers of certification reviews over the program's projected life cycle. Frequency of reviews should increase as the program nears the start of dedicated OT&E.
6		PM	Resolve open issues, particularly with requirements, sufficiently early to permit orderly planning and transition to dedicated OT&E.
7		PM, User	If an incremental strategy is used, a clear distinction exists between each increment for determining what is tested, produced and/or fielded. (See **Attachment 4**, **Attachment 10**)
8		PM	Operational capabilities are clearly assigned to specific increments.
9		PM	Provisions exist for developing and operationally testing subsequent increments after the initial increment is complete.
10		PM	Contract(s) capture the content of the most recent CRD or appropriate requirement document.
11		PM	CDT has been identified (if an ACAT 1 or MAIS program), or a TM (or CDT) for other than MDAP and MAIS programs.

12		PM	Systems Security Working Group (SSWG) (or equivalent) is formed with membership including representatives from the LDTO, OTO, and cybersecurity test agency(s).
Primary References: DoDI 5000.75, *Business Systems Requirements and Acquisition* DoDI 5000.80, *Operation of the Middle Tier of Acquisition (MTA)* DoDI 5000.81, *Urgent Capability Acquisition* DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 DAG AFI 63-101/20-101 AFI 99-103 AFI 10-601			

Attachment 3

ANALYSIS OF ALTERNATIVES (AOA)

Table A3.1. Analysis of Alternatives (AOA).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	The AoA (if necessary) may require updating, re-validation, and approval at the appropriate level prior to each milestone.
2		User	All reasonable alternatives are objectively described. The military value of the final alternatives are clearly identified.
3		PM	All relevant costs are identified, preferably using objective engineering and business estimates derived from accepted DAF cost analysis principles and processes.
4		PM	Cost Capability Analysis has been completed.
5		User	All assumptions and constraints are explicitly identified and supported by the latest CRD, AoA guidance documents, or reasonable basis determined by the AoA sponsoring agency.
6		User	Acceptable ranges of performance are established using rigorous cost-benefit, trade-off, and sensitivity analyses to show decision makers when and where certain degradations in system cost or performance yield outcomes that no longer satisfy the mission need.
7		OTO	Measures of Effectiveness (MOE) and Measures of Suitability (MOS) reflect operational utility and show how they were derived from the requirements documents.
8		OTO	MOEs and MOSs at the operational task level are "testable" in order to develop DT&E and OT&E plans and concepts. MOEs are developed as early as possible and agreed to between user and tester.
9		OTO	The AoA's MOEs, MOSs, Measures of Performance (MOP), and other criteria are linked to system performance thresholds stated in the latest threat and requirements documents and "track" throughout the program's development.
Primary references: DoDI 5000.84, *Analysis of Alternatives* AFI 10-601			

Attachment 4

CAPABILITIES REQUIREMENTS DOCUMENTS (CRD)

Table A4.1. Capabilities Requirements Documents (CRD).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	The appropriate CRD (e.g., Initial Capability Document (ICD), Draft Capability Development Document (CDD)), and CONOPS are coordinated and approved at appropriate levels prior to each milestone, after major program changes, and early enough to develop the TEMP, DT&E plan, OT&E concept, and OT&E plan.
2		User	AF Forms 1067, *Modification Proposal*, issued for modification programs that introduce a new capability, include a Table of Performance Parameters/Attributes (KPPs, KSAs, or other attributes) with minimum Threshold/Objective values similar to the format for a CDD. The vetted AF Form 1067 document serves as the CRD for sustainment modifications.
3		User	AF Forms 1067 issued for permanent sustainment modifications should identify CDD requirements the modification is intended to sustain.
4		User	The CRD is based on the Joint Planning Guidance, Joint Vision, Air Force Vision, USSF Vision, and long-range planning inputs from Joint, Air Force, and USSF CONOPS.
5		PM	The CRD's capabilities accurately flow down through the AoA, acquisition strategy, TEMP, DT&E plan, OT&E concept, and OT&E plan.
6		PM	The proposed system design satisfies projected operational requirements in the CRD and Strategic Planning Guidance.
7		PM	The system provides the needed capabilities against the most current validated threat described in the system's threat documents.
8		PM	Modeling and Simulation (M&S) requirements are identified early to enable programmed funding. (See **Attachment 17**)
9		User	Cyber threats, attack surfaces, and security requirements are current. Reference *DoD Cybersecurity T&E Guidebook* for details.

10		PM	Cyber requirements are achievable, testable, and measureable, and are derived from MBCRA results. Requirements should drive the development of a secure and cyber survivable system.
11		PM	Joint, multi-national, multi-departmental, or multi-service uses described in the CRD are addressed during the system's development.
12		User	All thresholds and objectives are stated in operational terms and defined in measurable, beneficial increments of capability.
13		User	Measureable and testable criteria for how the system supports military operations, is entered and managed on the network and how effectively it exchanges information is specified with threshold and objective values in accordance with the Joint Capabilities Integration and Development System (JCIDS) Net-Ready requirement.
14		PM	Cyber resiliency are addressed through the JCIDS Survivability KPP and by addressing the 10 Cyber Survivability Attributes.
15		User	CRDs are stated in such a manner that testable MOEs, MOSs, and MOPs are quantitatively measurable through analytically-based evaluation methods when possible.
16		User	All CTPs, KPPs, MOEs, MOSs, MOPs, threats, definitions, and other criteria are consistent (harmonized) across the most current support documents (e.g., CRD, system threat assessment, AoA, CONOPS, Acquisition Program Baseline, TEMP).
17		User	If increments of operational capability are planned, the CDD are updated to describe the next increment prior to development of the DT&E plan, OT&E concept, and OT&E plan.
18		User	Changes are finalized and open issues resolved early enough to prevent no adverse impacts on the successful completion of dedicated OT&E.
19		User	The CRD contains a complete audit trail documenting rationale for all requirements changes, including changes from the Acquisition Program Baseline.
20		User	Only systems with requirements to “protect users in combat” according to 10 USC § 2366 are listed as “covered systems.”
21		User	The CRD states the appropriate cybersecurity impact values (High, Moderate, and Low) for Confidentiality, Integrity and Availability as well as listing the appropriate security overlays as described in DoDI 8510.01.
Primary references:			

DoDI 5000.85
DoDI 8500.01, *Cybersecurity*
DoDI 8510.01
DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*
DoD Cybersecurity T&E Guidebook
CJCSI 5123.01H, *Charter Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System*
AFI 10-601
AFI 99-103

Attachment 5

THREAT & INTELLIGENCE DOCUMENTS

Table A5.1. Threat & Intelligence Documents.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	Threat assessment document(s) are valid and current with updates made prior to each milestone.
2		OTO, PM	Address program impacts of testing against emerging threats which may not be stated in the current validated CRD including cyberspace threats and impacts.
3		User	The system threat assessment document are approved by AF/A2. Defense Intelligence Agency validates the Validated On-line Life-cycle Threat (VOLT) for ACAT ID or IAM programs; the AF validates the VOLT for ACAT IC or IAC programs and below.
4		User	The system's threat assessment document(s) are consistent with current DoD threat projections and accurately reflected in the CRD and AoA.
5		PM	Sufficient threat details are provided to support system research and development, procurement of threat-representative systems necessary for testing, SE, and the development of realistic operational mission scenarios in support of the DT&E plan, OT&E plan, and schedules.
6		PM	All threats are described in system-specific terms and include system-to-system interfaces.
7		PM	Threat shot doctrine and employment tactics are described.
8		PM	The reactive threat and potential countermeasures are described.
9		PM	Sources for projections and areas of uncertainty are cited.
10		PM	Adversarial cyber capabilities and tactics are understood and described, such as using the MRAP-C.
11		PM	Life cycle mission data plans should be established by the program office, or its predecessor organization, for each IMD-dependent acquisition program and effort beginning at MS A.
Primary References: DoDD 5250.01 DoDI 5000.86, *Acquisition Intelligence* DoDI 5129.47, *Center for Countermeasures* CJCSI 5123.01H AFI 10-601 AFMAN 14-401, *Intelligence Analysis and Targeting Tradecraft / Data Standards*			

Attachment 6

INTEGRATED TEST TEAM (ITT) STANDUP & ITT CHARTER

Table A6.1. Integrated Test Team (ITT) Standup & ITT Charter.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	New-start programs direct establishment of an ITT in the initial Acquisition Decision Memorandum as soon as possible after the Materiel Development Decision. (Every program requires an ITT regardless of how long the program has been in existence.)
2		PM	A current ITT Charter describes ITT activities, membership, goals, products, responsibilities, and operating procedures.
3		PM	A CDT is identified for MDAP and MAIS programs, or a TM (or CDT) for all other programs. The CDT and the OTO representative co-chair the ITT.
4		PM	The charter covers the entire life cycle of the program.
5		PM	If the system comes under an overarching ITT of related systems, the ITT Charter includes provisions for managing multiple systems.
6		PM	All program stakeholders are represented (e.g., other services, interoperable systems, and organizations supporting all types of T&E activities).
7		PM	The ITT has sufficient membership participation to be effective.
8		ITT	The ITT directs formation of sub-groups to address specific tasks and responsibilities.
9		ITT	Research is completed to nominate an LDTO to the PEO for coordination and submittal to AFMC/A3 or USSF/TE for approval.
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 DAG AFI 99-103			

Attachment 7

CONCEPT OF OPERATIONS (CONOPS)

Table A7.1. Concept of Operations (CONOPS).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	The CONOPS describes expected system employment and operating concepts, strategies, methods, and tactics in concert with the latest CRD. Sufficient detail permits early development of operationally realistic test scenarios and tactics for the OT&E test concept and test plans.
2		User	Operational effectiveness and suitability requirements, criteria, thresholds, objectives, and definitions in the CRD accurately flow down from the CONOPS.
3		OTO	The OT&E test concept and OT&E plan are linked to the CONOPS.
4		User	Changes in the CRD, system threat assessment document, AoA, logistics support concepts (LSC), and TEMP are analyzed for potential impacts on CONOPS, which in turn affect T&E plans.
5		User	Changes in the CONOPS are finalized and open issues are resolved early enough to prevent no adverse impacts on the successful completion of DT&E, integrated testing, cyber T&E, and dedicated OT&E.
6		User	CONOPS are available to support development of operationally relevant DT&E and OT&E scenarios.
Primary References: CJCSI 5123.01H AFI 10-601 AFI 10-401, *Air Force Operations Planning and Execution*			

Attachment 8

LIFE CYCLE SUSTAINMENT PLAN (LCSP)

Table A8.1. Life Cycle Sustainment Plan (LCSP).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	The LCSP describes the optimal system maintenance strategies, concepts, and methods based on the CRD's requirements.
2		PM	The system uses an acceptable inter-Service, organic, and/or contractor mix.
3		User	The LCSP identifies potential high-risk and problem areas (such as TOs, system reliability, support equipment, and training).
4		PM	The LCSP identifies potential high-risk and problem areas from long lead items.
5		User	Logistics and readiness criteria, thresholds, objectives, and definitions in the CRD accurately flow down (be linked) from the LCSP.
6		OTO	The OT&E concept and plan should link the LCSP to the MOEs and MOPs.
7		User	LCSP strategies and plans are sufficiently detailed to support early development of the OT&E concept and OT&E plan.
8		OTO	Realistic operational and suitability test scenarios that support the integrated test plan are developed from the LCSP and other Air Force, and USSF concepts.
9		PM	The system is supportable in dedicated OT&E using the LCSP's strategies and plans.
10		PM	The system's design successfully addresses the quantitative and qualitative constraints identified in the LCSP.
11		OTO	The doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) elements are sufficient to support the LCSP and maintenance plan during dedicated OT&E.
12		PM	The Depot Source of Repair decision has determined the optimal maintenance posturing decisions needed to support warfighter operational requirements.

13		PM	Reliability and maintainability growth plans are developed, coordinated, and documented in the Systems Engineering Plan (SEP) and TEMP.
14		PM	The LCSP integrates the acquisition and product support strategies throughout the system's life cycle. The LCSP supports Milestone B and follow-on decisions. **Note:** Satellites are exempt from this requirement.
Primary References: DoDI 5000.85 AFI 63-101/20-101 *DoD Guide for Achieving Reliability, Availability, and Maintainability*			

Attachment 9

INFORMATION TECHNOLOGY (IT) & NATIONAL SECURITY SYSTEMS (NSS)

Table A9.1. Information Technology (IT) & National Security Systems (NSS).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	The SS KPP and Net Ready Performance Attribute prescribed in the CRD consists of testable characteristics and contains performance measures necessary for the timely, accurate, and complete exchange and use of information.
2		User, PM	Architecture products needed by Enclosure A and B of the CJCSI 5123.01H (e.g., OV-5, OV-6, and SV-1 to SV-7) are developed and available to the test community.
3		PM	Cybersecurity capabilities are planned and designed into system specifications and configurations using the latest threat estimates.
4		PM	An Authorizing Official and Information System Security Manager are formally assigned in writing.
5		User	Impact values for Confidentiality, Integrity and Availability as well as a listing of the security overlays are in requirements documents and the TEMP. (User) (See **Attachment 4**)
6		PM	The cybersecurity strategy, as an appendix to the Program Protection Plan (PPP), is complete and available to the T&E community. (See **Attachment 12**)
7		PM, LDTO	RMF and MRAP-C are implemented and the T&E community invited to observe and participate in process activities.
8		User	The High Performance Team's architecture expert checked the compliance with the DoD Information Enterprise Architecture.
9		PM	The Information Support Plan (ISP), Security Classification Guide, MRAP-C Report, and all RMF related documents (including a compiled list of system characteristics or qualities required for system registration, key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan) are complete, consistent with the TEMP, and available to the T&E community as early as possible.

10		PM	System cybersecurity training for Authorizing Officials, Information System Security Managers, security systems administrators, and users is available and completed.
11		LDTO	Trained teams are used to conduct passive and active scans to reveal system/network vulnerabilities, verify system protection and detection capabilities, and complete a Network Risk Assessment or equivalent as outlined in the TEMP and ISP.
12		PM, LDTO, JTIC	Network Risk Assessment and other interoperability or net-ready certification activities are complete.
13		PM	All developer passwords, test passwords, password scripts, and accounts in use during system development are deleted prior to operational testing.
14		PM, LDTO	Compliance with cybersecurity vulnerability alerts do not impact any other type of system certification or potentially invalidate test data.
15		PM	Data passed to and from other interoperable systems are compatible.
16		PM, JITC	JITC has provided an OTRR Interoperability Statement.
17		PM	The Authorizing Official has obtained an Authorization to Operate (ATO) memorandum or an Authorization to Operate With Conditions memorandum (as appropriate) prior to OT&E efforts.
18		PM	Systems and subsystems comply with the USAF Electromagnetic Compatibility Program and Radio Frequency Spectrum Management guidelines. (DoDI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*)
19		PM, OTO	Other interoperable systems and subsystems test articles (including external systems) are available. (See **Attachment 31**)
20		PM	Hardware and software vulnerability testing is complete and available to the T&E community.
Primary References: DoDI 5000.75 DoDI 5000.87 DoDI 5000.82, *Acquisition of Information Technology (IT)* DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)* DoDI 8500.01 DoDI 8510.01			

CJCSI 5123.01H
AFPD 17-1, *Information Dominance Governance and Management*
AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*
AFPAM 63-113, *Program Protection Planning for Life Cycle Management*
DoD CIO Memorandum, *DoD Information Enterprise Architecture*, Version 2.0
National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev 4
Joint Staff Cyber Survivability Endorsement Implementation Guide (CSEIG), V2.0

Attachment 10

TEST & EVALUATION MASTER PLAN (TEMP)

Table A10.1. Test & Evaluation Master Plan (TEMP).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	The TEMP is updated, coordinated, and approved at appropriate levels prior to each milestone and after major program changes.
2		PM	Open issues are addressed and resolved before submission to HQ USAF. Changes by OSD or other decision authorities are incorporated as agreed.
3		PM	Coordination is timely and efficiently planned to minimize chances of late rejection and negative impacts on dedicated OT&E.
4		PM	Level of detail is appropriate for the stage of development, and "To Be Determined (TBD)" eliminated as much as possible. MOEs, MOSs, CTPs, COIs, and decision support questions are included in the Developmental Evaluation Framework Matrix.
5		PM	The TEMP accurately reflects the most recent CRD, system threat assessment documents, LSC, Air Force, USSF concepts, and AoA.
6		PM, OTO	The TEMP clearly summarizes relationships between: 1) the strategy for T&E, program schedule, and resources; 2) CRD parameters, COIs, CTPs, MOEs, MOSs, and 3) Developmental Evaluation Framework, KPPs, CTPs, KSAs, Failure Modes, Effects and Criticality Analysis, interoperability requirements, cybersecurity requirements, reliability growth, maintainability attributes and developmental test objectives, other evaluation criteria, and decisions supported.
7		PM, OTO	The OT&E concept and plan are executable in terms of structure, schedule, and resources.
8		PM	The T&E schedule clearly articulates when contractor, integrated contractor-government, government developmental, integrated government developmental-operational, and government operational test occurs. This includes both functional and cybersecurity test events.
9		PM	The TEMP clearly delineates test responsibilities between contractor and the government.

10		PM	The requirements strategy (as reflected in the ICD and draft CDD) and acquisition strategy are fully supported (manpower, funding, test infrastructure, articles including M&S, and agencies). (see **Attachment 2**)
11		PM. OTO	T&E test resource shortfalls or limitations potentially impacting dedicated OT&E are identified.
12		PM. OTO	Describe the M&S assets needed for dedicated OT&E.
13		PM, OTO	The VV&A process and agency responsibilities are described for each M&S capability, to include expected products and approvals. (See **Attachment 17**)
14		PM	If LFT&E is directed, include the LFT&E strategy in the TEMP. (See **Attachment 16**)
15		PM	Appropriate cybersecurity test measures included to evaluate requirements from the SS KPP including the 10 CSAs and the operational capability to prevent, mitigate, and restore to sustain continuity of operation.
16		PM	Appropriate resilience and survivability testing is described in the TEMP to address system threats (See **Attachment 5**), even for non-covered systems. Testing should address resilience and survivability measures of the system, as well as potential failure and recovery modes.
17		PM	The TEMP describes what DT&E, OT&E, or integrated test has done or does to check the system meets the operational requirements in dedicated OT&E, including assessing schedule and product risks with requisite margins, and assessing mitigation plans of above.
18		OTO	Show how all COIs and measures are addressed in dedicated OT&E.
19		ITT	Contractor-conducted vs government-conducted DT and OT are clearly distinguished and mutually supportive.
20		PM	Rationale and provision are made for any planned OT&E deferred beyond dedicated OT&E into Follow-On Operational Test and Evaluation (FOT&E) or follow-on increments.
21		PM	Links to vital detailed information cited in the TEMP are functional and the linked information is complete.
22		PM	Reliability growth curves and planning.

23		PM, LDTO, OTO	Scientific Test and Analysis Techniques (STAT) calculations and analyses.
24		PM	Allocation of reliability among key components.
25		PM, LDTO	Anticipated development and test problem areas.
26		PM	Resolution of past deficiencies.
27		LDTO, OTO	Cyber T&E Strategy (CTES), informed by the MBRCA (e.g., MRAP-C), includes: cyber threats, architecture, operational environment, evaluation structure, ATO requirements, test event schedule, test resources (to include who performs cybersecurity testing), and how each of the cybersecurity test phases are accomplished. Identify prior cybersecurity test events that impact planned cyber DT and/or OT.
28		LDTO, OTO	Developmental Cybersecurity testing (cooperative vulnerability identification and adversarial cybersecurity assessment) events for DT&E and/or integrated test are described. Developmental Evaluation Framework (DEF) includes rows for cybersecurity (e.g., confidentiality, integrity, and availability) and cyber resiliency (e.g., protect, mitigate, and recover), and identifies which cybersecurity test activities are accomplished to assess each area to inform the applicable Decision Support Questions (DSQs)
29		LDTO, OTO	Operational Cybersecurity testing (cooperative vulnerability and penetration assessment and adversarial assessment) events for OT&E and/or integrated test are planned.
30		PM	RMF and MRAP-C planning is described.
31		PM	The TEMP includes applicable test scenarios, appropriate data collection (established common T&E database), and performance evaluation over the life cycle of the system.
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 DAG AFI 99-103 AFI 63-101/20-101			

DAFPAM 63-128, *Integrated Life Cycle Management*
DoD Cybersecurity T&E Guidebook

Attachment 11

INTEGRATED TEST PLANNING

Table A11.1. Integrated Test Planning.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM, LDTO, OTO	Integrated test planning starts as early as practical to make T&E schedules and resource expenditures more efficient and eliminate duplication of effort.
2		PM	A rigorous SEP identifies how T&E is used to achieve program goals and technical results.
3		PM	The TEMP specifies how T&E is planned and used to verify and validate program requirements so the system is operationally effective and suitable. (See **Attachment 10**)
4		ITT	DT&E and OT&E plans and concepts are structured and shared among the ITT early so the OT can capture and apply DT&E test procedures and data to enable integrated test planning and reduce OT&E timelines and requirements. (See **Attachment 13**, **Attachment 14**, **Attachment 23**, **Attachment 25**)
5		PM, OTO	OAs may be accomplished at any time in the development program. OAs and early user inputs influence system design and function. (See **Attachment 10**)
6		PM	Other types of T&E (e.g., cybersecurity, LFT&E, contractor) are incorporated as much as practical in the integrated test design.
7		ITT	Dedicated OT and DT objectives are not compromised.
8		LDTO, OTO	STAT process employed so T&E is effective and efficient; and appropriate factors and conditions are selected to produce the data necessary to characterize system capabilities.
9		PM	The TEMP reflects the most current program direction.
10		ITT	Definitions, formulas, and evaluation criteria used to determine operational effectiveness and suitability are consistent between all individual test plans and T&E documents.
11		PM	A common T&E database for the program will be used to archive all T&E data from all test organizations.
12		ITT	Parameters and formats are agreed upon by all test teams.

13		PM	Test item configurations are rigorously controlled. (See **Attachment 18**, **Attachment 22**)
14		ITT	Integrated test matrices are addressed in the TEMP and depict all T&E events and who accomplishes them.
15		ITT	Duplication and voids in testing are minimized. (See **Attachment 22**)
16		PM	A prudent number of backup resources (e.g., test assets, funds) are available to supplement all testing if planned integrated DT&E and OT&E data is unusable or unavailable. (See **Attachment 22**, **Attachment 25**)
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 DAG AFI 99-103			

Attachment 12

CYBER RESILIENCY

Table A12.1. Cyber Resiliency.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		ITT	Cyber resiliency goes beyond "cybersecurity" to include cyberattack detection and response. Cybersecurity phases are reviewed for currency of the strategies for operational requirements, acquisition, T&E, and cybersecurity. Reference DoD Cybersecurity T&E Guidebook.
2		PM	System's Cybersecurity Strategy, Security Plan, Security Classification Guide, ISP, and PPP are current, including how they address the SS KPP and the 10 CSAs. Cybersecurity test strategy is based upon MBCRA and hands-on test findings.
3		ITT	Cyber resiliency assessments are integrated into DT&E and OT&E as described in the DoD Cybersecurity T&E Guidebook.
4		ITT	OT plan addresses necessary DOT&E cybersecurity content: TEMP linkage, architecture, intelligence community-validated cyber threat, operational environment, evaluation structure, time and resources, cooperative vulnerability and penetration assessment, and adversarial assessment. (See **Attachment 15**)
5		ITT	OT plan should also address cybersecurity software assurance considerations. (See **Attachment 15**)
6		PM	MRAP-C and Six-step RMF process (1. Categorize System, 2. Select Security Controls, 3. Implement Security Controls, 4. Assess Security Controls, 5. Authorize System, 6. Monitor Security Controls) are followed. Establish an ITT sub-group to monitor and control, if necessary.
7		PM	Confidentiality, Integrity, and Availability ratings as well as a listing of security overlays are properly assigned.
8		PM	Applicable overlays are applied so that appropriate security controls are selected and updated.
9		PM	Cyber-attack surfaces, threats, etc., are properly characterized and updated.
10		PM	Cyber kill chain is correctly understood, analyzed, and updated.

11		PM	The MRAP-C report is current and characterizes the cyberattack surface, identifies potential cyber vulnerabilities, identifies cybersecurity test resources, and informs cooperative and adversarial cybersecurity test events.
12		ITT	CTES and MRAP-C report are up to date. Each MRAP-C iteration incorporates the latest available architecture, mission, environment, and threat information.
13		PM	Cybersecurity test infrastructure (with appropriate architecture, level of realism, and security) and documentation is available and described in the TEMP.
14		PM	System owners and cybersecurity testers agree on rules of engagement for testing.
15		PM	Reciprocity agreements are in place between teams and other Services.
16		ITT	Test plans with refined cyber T&E scenarios, operational capability requirements, potential test venues, mission threads, and simulated scenarios are developed and approved.
17		PM	Funding is available to complete cooperative vulnerability and penetration assessment, and adversarial assessment test events.
18		PM	The ATO or an ATO with Conditions are available at the appropriate times, usually pre-Milestone C.
19		PM	Security Assessment Report is prepared, recommended corrective actions and system weaknesses are addressed and prepared for.
20		PM	All cybersecurity testing planned to be conducted on a cyber range is identified and all events integrated with OT&E and assessment activities.
21		PM	All necessary linkages between the cyber range and operational networks are developed.
22		PM	Integration plan established for system users, network defenders, and threat emulations on planned cyber range if conducting cyber range testing.
23		PM	DT and OT cybersecurity test events are sufficient to fully assess the system’s cyber resiliency when exposed to representative cyber threats. The cyber vulnerabilities and potential mission impacts during the MRAP-C informs cybersecurity test event prioritization.

24		PM	MBCRAs (e.g., MRAP-C) have been conducted to characterize the cyberattack surface, identify potential cyber vulnerabilities, identify cybersecurity test resources, and to inform: Milestone and Authorization to Proceed decisions, cyber requirements identification, systems engineering technical reviews, and cooperative and/or adversarial cybersecurity test events.
25		PM	CTES has been developed and updated based upon MBCRA (e.g., MRAP-C) results. Each MBCRA iteration incorporates the latest available architecture, mission, environment, and threat information.
26		PM, OTO	Cooperative vulnerability and penetration assessment and adversarial teams are available and scheduled.
27		PM, OTO	Testability of cyberspace requirements are determined and additional clarification received as needed.
28		OTO	Applicability of network defender participation in adversarial assessment team OT&E events is determined.
29		OTO	Limitations of generating operational effects during cybersecurity adversarial assessment OT&E events due to safety and real-world operations considerations are identified and documented.
30		OTO	Qualitative cyber resiliency factors, descriptors and tailored measures are identified.
31		OTO	The threat basis for vulnerability and penetration testing is identified and documented in the test concept and scenarios.
32		OTO, PM	Resources are allocated to cybersecurity test events.
33		PM, LDTO	Identify security constraints and their impacts on dedicated OT&E.
34		PM, LDTO	Receipt of permissions and rules of engagement before the cooperative vulnerability identification and the adversarial cyber DT&E events.
35		PM, LDTO	Cyber anti-tamper testing is integrated into DT&E and OT&E to the extent warranted and permissible.
36		PM	System OPSEC plan is current.
37		PM, ITT	If National Security Agency certification is required for classified and controlled cryptographic items, the program's security verification test approach are included in the TEMP.
38		PM	Cyber vulnerabilities identified during MBCRAs (e.g., MRAP-C) and/or cybersecurity testing which can result in a Category

			(CAT) I or CAT II deficiency condition are tracked accordingly in the programs Deficiency Reporting system.

Primary References:
DoDI 5000.75
DoDI 5000.82
DoDI 5000.85
DoDI 8500.01
DoDI 8510.01
CJCSI 5123.01H
CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*
CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*
NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-57, *Recommendation for Key Management, Parts 1, 2, and 3*
NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*
DoD Cybersecurity T&E Guidebook
SS KPP CSEIG Vol I and Vol II
DAG
AFI 99-103

Attachment 13

CONTRACTOR TESTING

Table A13.1. Contractor Testing.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	All system specifications and contractor requirements support the latest CRD.
2		PM, C	Comprehensive contractor test plans for development, qualification, and production acceptance testing are in place.
3		C	Requirements and specifications flows down accurately and clearly from prime contractors to subcontractors in accordance with the contract terms.
4		PM, LDTO	Contractor test strategies and methods support the premise that all aspects of the specification and the CRD can be met.
5		C	Test events should be performed with operationally relevant components and elements under operationally relevant conditions and scenarios as much as possible with exceptions agreed to by all stakeholders and/or limitations cited.
6		PM	Sub-system and system pass/fail specification thresholds are directly traceable to the most current CRD.
7		C	A realistic, attainable, event-driven test schedule is proposed, evaluated, and funded.
8		C	Known risks are reasonably and appropriately managed.
9		PM	All contractor test data is available in the system's common T&E database. Additionally, PMs should request contractors provide documentation to enable the extraction and analysis of the data by DT and OT personnel.
10		PM	Contractor testing is described in the TEMP. (See **Attachment 10**, **Attachment 11**)
11		PM	The contractor is capable to plan and conduct special and formal multi-segment and system of system testing, including test support, handling, calibration, and transportation.
12		C	Contractor testing demonstrates the system and/or components are meeting the CTPs at prescribed threshold levels and within defined time frames at each step in development.

13		LDTO	Government systems engineering analysis should determine if test results support achievement of the specification and if the system is projected to meet operational requirements.
14		C	Fault tree analysis is performed on the operational system and its external and internal interfaces to identify potential operational contributors to mission failure.
15		PM	Available government facilities are used in contractor testing wherever cost-effective, available, and feasible.
16		PM, C	A deficiency resolution system is in place and accessible to all test organizations to identify, track, and resolve test failures. (See **Attachment 19**)
17		PM	The contractor's DR process is compatible with the government's DR process. (See **Attachment 19**)
18		PM	All test failures and resultant system design changes are documented and analyzed for effectiveness. Tests are repeated as necessary to certify specification compliance.
19		PM	Document all changes to specification threshold (pass/fail) values and rationale.
20		PM	Contractor T&E data and information are available in the required formats for government review for impacts on DT&E and dedicated OT&E.
21		C	Planned contractor testing is completed according to the contract before government acceptance and dedicated OT&E.
22		PM	Any contractor testing deferred beyond government acceptance of the system requires complete approval of the contract modification prior to government acceptance and should be well-defined for final mission-oriented test readiness certification.
23		PM, C	Contractor cybersecurity testing incorporates testing of potential cyber vulnerabilities identified during integrated MBCRA (e.g., MRAP-C) events conducted before and during system development. Cybersecurity test results are made available to the government to review for system design changes as well as for potential impacts on DT&E and dedicated OT&E.
Primary References: DoDI 5000.02T DoDI 5000.75 DoDI 5000.81 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89			

DAG
AFI 99-103
TO 00-35D-54, *USAF Deficiency Reporting, Investigation, and Resolution*
Incorporating Test and Evaluation into Department of Defense Acquisition Contracts

Attachment 14

GOVERNMENT DEVELOPMENTAL TEST & EVALUATION (DT&E)

Table A14.1. Government Developmental Test & Evaluation (DT&E).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	CRD requirements are accurately reflected in government DT&E plans and can be demonstrated during contractor and government DT&E.
2		PM	When design-cost-performance trade-offs are made that may impact CRD requirements, user concurrence is obtained and documented where appropriate.
3		PM	Provide a safety release for the system prior to each DT. (See **Attachment 23**)
4		LDTO	Reviewed and validated the program office risk assessments for hazards that were not eliminated through redesign and provided the using commands with their recommendations on program office risk assessments. (See **Attachment 23**)
5		PM	The DT&E schedule and testing are planned and executed to allow sufficient time to certify system OT&E readiness, start and complete dedicated OT&E before FRP or fielding.
6		PM	DT&E, with inputs from LDTO, validates contractor testing is complete, or a contractually approved plan exists to finish testing. (See **Attachment 13**)
7		LDTO	Sufficient suitability testing is conducted to permit credible predictions about system Reliability, Maintainability, and Availability. (See **Attachment 8**)
8		PM	All CTPs demonstrates satisfactory performance, or supported by reliability growth plans and/or curves that show threshold attainment.
9		LDTO	The LDTO has provided the program office a summary of the test hazards and the mitigating actions for all serious and high test hazards.
10		PM	A government-run DR system is in place in support of DT&E and OT&E for identifying, tracking, reporting, and resolving DRs. (See **Attachment 19**)

11		PM	Correction of all CAT I deficiencies including cybersecurity vulnerabilities identified during DT blue team and red team events are implemented before start of dedicated OT&E. (See **Attachment 19**)
12		PM	A formal process is in place to control and track system configuration during DT&E that supports dedicated OT&E. (See **Attachment 18**)
13		PM	The system design is stabilized sufficiently early with no major changes implemented in the OT&E test articles. (See **Attachment 18**, **Attachment 19**, **Attachment 21**)
14		LDTO	Sufficient operationally relevant DT&E is accomplished to determine if CRD requirements can be met before dedicated OT&E.
15		PM, LDTO	Cooperative vulnerability identification and adversarial cyber DT&E are complete.
16		PM, LDTO, JITC	Sufficient testing is accomplished with other systems to support end-to-end cybersecurity and interoperability certifications. (See **Attachment 9**, **Attachment 12**)
17		PM	If the system configuration has changed from the previously documented baseline, provide updated configuration diagrams and documentation to support testing activities.
18		PM	Levels of performance are demonstrated in the intended operational environment based on the CRD, CONOPS, strategies, and plans. (See **Attachment 21**)
19		PM	Sufficient workarounds acceptable to the user and OTO are identified for CAT II vulnerabilities and deficiencies.
20		PM	If there are interoperability requirements, DT&E takes place at the system-of-systems level. (See **Attachment 9**)
21		PM	LFT&E results (if required) are available before start of dedicated OT&E. (See **Attachment 16**)
22		PM	Resilience and survivability results (as appropriate) are available before the start of dedicated OT&E for non-covered systems.
23		PM	Appropriate documentation is available from the following sources, when applicable (among others): (1) Non-nuclear Munitions Safety Board; (2) Directed Energy Weapons Safety Board; (3) Flight Safety Board; (4) Airworthiness, Space Flight Worthiness; (5) Range Safety; (6) Nuclear Weapons Center; (7) Institutional Review Board for Protection of Human Subjects in Testing; (8) SEEK EAGLE certification completed for threshold

			systems as a minimum; (9) AF Spectrum Management Office; (10) ATO; (11) Space and Orbital Safety; (12) Communication, Navigation, Surveillance/Air Traffic Management (CNS/ATM) Letter of Compliance; (13) Military Flight Operations Quality Assurance. (See **Attachment 23**)
24		LDTO, OTO	For integrated testing, minimize duplication and voids in testing and the excessive use of facilities. (See **Attachment 10**, **Attachment 11**, **Attachment 13**, **Attachment 22**, **Attachment 32**)
25		LDTO, OTO	DT&E data formats and parameters are compatible with other tests to maximize data availability in the common T&E database and usability for OT&E. (See **Attachment 11**)
26		PM	An agreed-upon plan and rationale exists (e.g., in the TEMP) for testing any areas or capabilities deferred past the start of dedicated OT&E.
27		LDTO	If there are any incomplete test areas, explain why and give impacts on dedicated OT&E with inputs from the OTO.
28		LDTO	Sufficient interim DT&E results and evaluations are available to support certification of readiness for operational testing. (See **Attachment 13**)
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 DAG AFI 99-103 AFI 63-101/20-101			

Attachment 15

SOFTWARE DEVELOPMENT & MATURITY

Table A15.1. Software Development & Maturity.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	System software functionality, performance, and maturity are assessed throughout the systems engineering technical reviews from Systems Readiness Review through Mission-Oriented Test Readiness Certification and developmentally tested at the full system level (suitable for that increment) prior to starting dedicated OT&E. (See **Attachment 21**)
2		PM	Define software-related exit criteria for MS B. These criteria may be modified and/or criteria added and/or deleted in response to CRD changes during system development.
3		PM	Develop and implement a "requirements traceability" metric to measure adherence of software products (to include architecture, design, and code) to the CRD. (See **Attachment 4**)
4		PM	Operational databases are complete and sufficient for operational test and contain actual operational data.
5		PM	System level integration testing of software and hardware-software-firmware interfaces are monitored, documented, and completed. (See **Attachment 31**)
6		PM	Effective software configuration management and control procedures are in place. (See **Attachment 19**)
7		PM	Software manuals and documentation are validated and up-to-date with the current software baseline in support of dedicated OT&E. (See **Attachment 31**)
8		PM	Software and firmware configurations are fully documented and frozen before starting dedicated OT&E. Changes implemented during dedicated OT&E impact the configuration being fielded or produced. (See **Attachment 18**)
9		PM	Incrementally deployed software releases that address specific capabilities and testable performance requirements are assessed ready for test.
10		PM	Each release underwent dedicated OT&E. Software builds or increments that are not deployed individually (release) still support full deployment system OT&E.

11		PM	The software is stable (i.e., operate error free for a reasonable length of time prior to dedicated OT&E). (See **Attachment 21**)
12		PM	Facilities, tools, and manpower are sufficiently representative to support the OT&E plan and schedule, and fielding of the software. (See **Attachment 8**, **Attachment 25**)
13		PM	Required Software Assurance Defense Information Systems Agency (DISA) Security Technical Implementation Guide and CNSSI-1253 controls and protection mechanisms are identified, implemented, and tested to prevent system compromise, maintain integrity and availability, and prevent unauthorized access to systems and data.
14		PM	Used automated vulnerability analysis tools & techniques throughout the lifecycle.
15		PM	Determine appropriate remediation strategies for all identified Required Software Assurance vulnerabilities.
16		PM	For critical software, employed independent Required Software Assurance Verification & Validation (V&V) organizations through DT.
17		PM	Known software and firmware vulnerabilities, exploitability levels, and discrepancies affecting system performance or the dedicated OT&E are properly documented and appropriate corrective action(s) taken. (See **Attachment 19**)
18		PM	The software is analyzed for safety critical functions.
19		PM	Any residual safety risks and hazards not eliminated through redesign should be included in the program office risk assessments.
20		PM, LDTO	Sufficient regression testing is accomplished at the unit, integration, and system-of-systems level so changes do not introduce operationally critical faults and/or result in additional defects.
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.89 DoDI 5000.87 TO 00-35D-54			

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*
AFI 16-1001, *Verification, Validation and Accreditation (VV&A)*
AFI 63-101/20-101

Attachment 16

LIVE FIRE TEST & EVALUATION (LFT&E)

Table A16.1. Live Fire Test & Evaluation (LFT&E).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Review the most current threats and operational scenarios in the CRD, threat documents, CONOPS, and AoA to assess whether program is or is not a "covered system."
2		PM	Consult AF/TEP, users, and OSD/DOT&E (in that order) for concurrence with the determination of covered system status.
3		PM	If the system is a covered system, determine LFT&E scope and complete a cost-benefit analysis.
4		PM	If full-up LFT&E is determined to be cost-effective and practical, develop an LFT&E strategy, to include the level of funding, and submit to AF/TE and subsequently to OSD/DOT&E for approval.
5		PM	Describe the LFT&E strategy in the TEMP and submit individual plans for "full-up system level" LFT&E to AF/TE and subsequently to OSD/DOT&E.
6		PM	Fully integrate the LFT&E strategy and plans into the overall strategy for T&E, TEMP, and integrated test plans. (See **Attachment 10**, **Attachment 11**)
7		PM	Plan for and fund LFT&E to be completed before start of dedicated OT&E.
8		OTO	Review and validate the program office risk assessments for hazards that were not eliminated through redesign and provide the using commands with their recommendations on program office risk assessments.
9		OTO	Provide the program office a summary of the test hazards and the mitigating actions for all serious and high test hazards.
10		PM	If full-up LFT&E is determined not to be cost-effective and practical, prepare an LFT&E waiver request and an alternate LFT&E plan for the MDA for PEO, SAF/AQ, AF/TE, and OSD/DOT&E approval before MS B. For programs that enter after MS B, prepare an LFT&E waiver request and an alternate LFT&E plan as soon as practicable for approval.

11		PM	Describe the alternate vulnerability and lethality strategy in the TEMP.
12		PM	Plan for and fund “alternate” LFT&E to be completed before start of dedicated OT&E.
13		PM	Deficiencies identified during LFT&E that are to be corrected are tracked and retested prior to certification for dedicated OT&E.
14		PM	Fully comply with all system-specific congressional direction regarding LFT&E.
15		User	For threat systems for LFT&E, the threat engagement doctrine and employment tactics reflect the contents in the CRD, CONOPS, and threat documents.
16		PM	For threat systems for LFT&E, the threat systems and threat models are VV&A’d before use in LFT&E. (See **Attachment 18**)
17		PM	For threat systems for LFT&E, identify limitations in the test threats and voids in covering the threat spectrum. Describe proposed fixes.
18		PM	For threat systems for LFT&E, where limitations exist in test threat systems, obtain approval to fill gaps with M&S and alternative systems.
19		PM	Develop a data reduction and common T&E database for using all validated threat test data throughout the integrated test plan.
20		PM	Provide a safety release for the system prior to each live fire test. (See **Attachment 23**)
Primary References: DoDI 5000.80 DoDI 5000.81 DoDI 5000.85 DAG AFI 99-103			

Attachment 17

MODELING & SIMULATION (M&S)

Table A17.1. MODELING & SIMULATION (M&S).

Note: Confirm the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		User	M&S requirements are identified in CRDs to obtain funding and support for their development or reuse. (See **Attachment 4**)
2		PM	Develop a Modeling and Simulation Support Plan that links M&S requirements to the capabilities being developed and tested throughout the program (from the AoA through the MS C decision). The Modeling and Simulation Support Plan can be part of existing program, engineering or technical plans.
3		PM	Identify as early as possible the M&S support requirements, to include funding, over the entire system life cycle.
4		PM	The Modeling and Simulation Support Plan address continuing ownership and maintenance of M&S assets after system fielding.
5		PM	Identify M&S linkages with planned interfacing and interoperable systems.
6		PM	Check for archived M&S tools before building new M&S resources.
7		PM	Programs obtained data and models for M&S from the authoritative sources when available and feasible.
8		PM	There is a plan for the government to take possession of any non-proprietary copy of models. Identify how those M&S resources are sustained.
9		PM	M&S assets, test tools, and analysis tools are available and usable for T&E. Testers received adequate training as necessary.
10		PM	M&S V&V plan and comprehensive schedule supports the integrated test plan and the dedicated OT&E plan and schedule.
11		PM	Scenarios, test tools, and analysis tools used for DT&E are adequately documented.
12		PM	The design engineering data is reviewed. Physics models can be objectively V&V'd, whereas operations analyses are subjectively

			V&V'd. Empirical test data should be used to establish model credibility.
13		OTO	Any M&S used to support dedicated OT&E is accredited.
14		OTO	If M&S generates results used to support a deployment and/or FRP decision on an OSD T&E Oversight program, OSD/DOT&E approves its use in dedicated OT&E.
Primary References: DoDI 5000.70, *Management of DoD Modeling and Simulation (M&S) Activities* DoDI 5000.85 DoDI 5000.86 AFI 16-1001 AFI 63-101/20-101			

Attachment 18

CONFIGURATION MANAGEMENT

Table A18.1. Configuration Management.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Configuration management is an established element of a program's systems engineering process.
2		PM	The systems engineering and configuration management process are used for all system components and support items (e.g., hardware, software, support equipment, spares, GFE). (See **Attachment 20**)
3		PM	A configuration control mechanism is used so the orderly transition from one decision review to the next, and from development to production.
4		PM	The government has sufficient oversight and understanding over the configuration to confirm changes do not invalidate the results of DT&E or dedicated OT&E. (See **Attachment 20**)
5		PM	Have a validated process that can trace and document the exact system configuration throughout its lifecycle.
6		PM	If known deficiencies remain in test articles before start of dedicated OT&E, the SEP describes strategies for managing the following areas: (1) System form, fit, and function are not adversely affected as a result of each deficiency correction; (2) the impacts of fixing before versus after dedicated OT&E is assessed; (3) all changes are documented and under configuration control. (See **Attachment 19**, **Attachment 20**)
7		PM, OTO	The system configuration and configuration of interfacing systems are stable and production representative before the start of dedicated OT&E. Once OT&E starts, configuration changes to the system under test are approved by the OTO. (See **Attachment 15**, **Attachment 20**)
Primary References: DoDI 5000.75 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 AFI 63-101/20-101			

Attachment 19

DEFICIENCY IDENTIFICATION & RESOLUTION PROCESSES

Table A19.1. Deficiency Identification & Resolution Processes.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		C	A contractor-operated DR process, if established, augments the PM's deficiency reporting process.
2		PM	The PM's deficiency reporting process is open to all stakeholders for promptly identifying, reporting, tracking, and resolving system deficiencies.
3		PM	A Material Improvement Project Review Board confirmed the resolution of all DRs and the impacts to dedicated OT&E are listed.
4		LDTO, PM	A Deficiency Review Board periodically reviews, validates, and prioritizes all open DRs.
5		PM	DRs should be rank-ordered, and the most critical worked first or as agreed by the user(s), operational tester, and LDTO.
6		PM, User, OTO	Open DRs from DT&E do not preclude successful conduct of dedicated operational testing and the achievement of operational requirements.
7		PM, OTO	Dedicated operational test results are not invalidated due to deferred DR resolution.
8		PM	The DR analysis process is complete and coordinated with users and testers prior to the start of dedicated OT&E.
9		LDTO, PM	Known DRs or capabilities deferred beyond the start of dedicated OT&E are reviewed and prioritized by a T&E Deficiency Review Board and an impact analysis performed.
10		PM	CAT I deficiencies are fixed and closure verified according to an agreed upon plan.
11		PM	CATtII deficiencies are fixed and closure verified, or suitable workarounds provided.
12		PM	For DRs that cannot be resolved prior to start of dedicated OT&E, a plan exists for testing deferred capabilities and fixes after dedicated OT&E is accomplished.
13		PM	The plan addresses how open DRs are tracked from increment to increment after OT&E is complete.

14		ITT	A Joint Reliability and Maintainability Evaluation Team and a Test Data Scoring Board are established to review all Reliability, Availability, and Maintainability data.
15		PM	Plan of Action and Milestones shows how cybersecurity DRs and vulnerabilities are resolved. (See **Attachment 12**)
Note: Review the phases shown in DoD Cybersecurity T&E Guidebook to verify currency of the strategies for requirements, acquisition, T&E, and cybersecurity. Primary References: DoDI 8500.01 DoDI 8510.01 DoD Cybersecurity T&E Guidebook DAG AFI 63-145, *Manufacturing and Quality Management* AFI 99-103 TO 00-35D-54			

Attachment 20

PRODUCTION & OPERATIONALLY REPRESENTATIVE TEST ARTICLES

Table A20.1. Production & Operationally Representative Test Articles.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Test articles (to include support equipment, Mission Planning System (MPS), software, and GFE) are production representative as possible or operationally representative to support the OT&E plan and schedule.
2		PM	Sufficient quantities of test articles to meet planned test objectives within an agreed-to schedule are available for functional and cyber OT&E.
3		PM, LDTO, OTO	Sufficient quantities of test articles to meet planned developmental and integrated test objectives within an agreed-to-schedule are available for functional and cyber DT&E.
4		PM	Test articles have achieved stabilized performance.
5		OTO	Test article requirements are provided as early as possible to guarantee sufficient lead time for procurement.
6		OTO	Where practical, aircrew and/or user carry-on equipment should mirror what is current with the users (e.g., aircrew flight equipment, electronic flight bag, night vision devices, other MPS hardware, etc.).
7		OTO	Assess any configuration differences between pre-production, production, or operationally representative test articles and the expected impact on the validity of OT&E.
8		OTO	Other interoperable systems and subsystems test articles (including external systems) are available, and of correct configuration, to permit testing in an operationally realistic manner. (See **Attachment 10**)
9		PM	The systems are production-representative or operationally representative.
10		PM	A process is in place to manage interoperability with other systems and subsystems. (See **Attachment 9**, **Attachment 18**)
11		PM, LDTO, OTO	Embedded test instrumentation is transparent to system performance and test execution.
Primary References: DoDI 5000.85 DoDI 5000.89 DAG			

Attachment 21

SYSTEM PERFORMANCE

Table A21.1. System Performance.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	At the conclusion of OT, the system demonstrated it is capable of meeting the CRD's requirements (i.e., is operationally effective and suitable) in its intended operational environment using operationally relevant scenarios.
2		PM, OTO	The PM and OTO should review the results of DT and IT test events and evaluate the system's progress and/or risk toward meeting MOEs, MOSs, MOPs, and other test criteria in (or derived from) the CRD.
3		PM	The system demonstrated it is on track to meet criteria for FRP and/or deployment decision.
4		ITT	The system demonstrated satisfactory performance and resiliency in contested environments.
5		PM	System DT&E demonstrated known functional and cyber deficiencies are identified and corrected, fixes verified, or otherwise resolved or deferred. (See **Attachment 19**)
6		PM	Any remaining problem areas are characterized and have minimal to no impact on the outcome of dedicated OT&E.
7		PM	All CTPs demonstrated satisfactory performance, or be supported by reliability growth plans and/or curves from the SEP that show suitability threshold attainment.
8		PM	System integration problems are corrected to allow Users to satisfy mission requirements. The system is ready for system- or mission-level testing.
9		PM	Integration among system components, subsystems, and external systems optimized total system design and performance capabilities, within known constraints.
10		PM	If the system was planned with an incremental acquisition strategy, describe what capabilities are lacking at this time and when they are implemented.
11		PM	Incremental acquisition strategy includes impacts to existing system as additional capabilities are incorporated.

12		PM	LFT&E (if required) are complete and achieve (acceptable) levels of system survivability or lethality. (See **Attachment 16**)
13		PM	Review results of any EOA or OAs accomplished and known deficiencies are identified and corrected, fixes verified, or otherwise resolved or deferred.
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 DAG AFI 99-103			

Attachment 22

OPERATIONAL TEST & EVALUATION (OT&E) PLAN

Table A22.1. Operational Test & Evaluation (OT&E) Plan.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		OTO	The OT&E test concept (if required) is developed and briefed to Mission-Oriented Test Certification Official as early as feasible (no later than 180 days before start of dedicated OT&E for non-rapid and/or non-agile programs on OSD oversight). (See **Attachment 11**)
2		OTO	The OT&E test concept is based on the characteristics of the operations and support environments, test equipment (to understand limitations or exceptions), and test scenarios the system encounters in dedicated OT&E.
3		OTO	The OT&E concept and OT&E plan are developed from the strategies in the LSC and other CONOPS. (See **Attachment 7**, **Attachment 8**)
4		OTO	The dedicated OT&E plan is developed, coordinated, and approved as early as feasible. For non-rapid and/or non-agile programs on OSD OT&E Oversight, OSD/DOT&E approved the adequacy of the test plan NLT 60 days prior to dedicated OT&E start.
5		OTO	A dedicated phase of rigorous, operationally realistic OT&E is planned.
6		OTO	Sufficiently realistic testing, to include realistic scenarios, emulate expected combat and peacetime environments.
7		OTO	COIs, MOEs, and MOSs clearly define linkages to the CRD, AoA, and threat documents and summarized in the TEMP.
8		OTO	The elements of operational suitability and all logistics support elements are addressed. (See **Attachment 8**, **Attachment 25**, **Attachment 26**, **Attachment 28**, **Attachment 31**, **Attachment 32**)
9		OTO	Open issues and disconnects (e.g., with test methodologies, common T&E databases, requirements, and MOEs) are resolved prior to OT&E start.

10		OTO	Definitions, formulas, models, scenarios, and evaluation criteria are standardized as much as possible between all test plans for the system. (See **Attachment 11**, **Attachment 14**)
11		OTO	For MOT&E, the OT&E plan is coordinated with the other Service OTAs and their inputs integrated into the lead OTO plan.
12		OTO	OT plan addresses DOT&E cybersecurity content: TEMP linkage, architecture, operational environment, evaluation structure, time and resources, cooperative vulnerability and penetration assessment, and adversarial assessment.
13		OTO	All T&E resources (e.g., M&S support, test articles, training, fault analysis, test facilities and ranges, contracting, cyber cooperative vulnerability and penetration assessment and adversarial assessment teams, and network defenders) are identified and scheduled. (See **Attachment 12**, **Attachment 23**, **Attachment 25**, **Attachment 26**, **Attachment 27**, **Attachment 28**, **Attachment 30**, **Attachment 31**, **Attachment 32**)
14		ITT	OT&E test plans are integrated (e.g., capitalize on the activities and data from other tests) as much as practical. (See **Attachment 10**, **Attachment 11**)
15		ITT, LDTO, OTO	OT&E test objectives are not compromised as a result of integrated testing.
16		LDTO	DT&E and other test data can supplement dedicated OT&E as much as possible.
17		OTO	Test item configurations are rigorously controlled and operationally representative. **Note:** Once the system is undergoing OT, any configuration changes should be approved by the OTO. (See **Attachment 18**)
18		OTO	The operational test plan is coordinated with other test organizations to avoid duplication and gaps in testing are minimized.
19		PM	A prudent number of backup resources (e.g., test assets, funds) are available to supplement dedicated OT&E if planned integrated test data is unusable or unavailable.
20		OTO	A plan exists for dry running test procedures.
21		OTO	The OT&E Test Plan addresses the identified program office and OTO test hazards and the mitigating actions for all serious and high test hazards.

22		OTO	All OT&E limitations are described (e.g., lack of test articles, time, system capabilities, insufficient operational realism) that may impact the FRP or deployment decision.
23		OTO	Describe how these limitations (and any waivers) are addressed in subsequent increments, FOT&E, FDE, and beyond.
24		User	Threat "shot doctrine" and employment tactics accurately reflect CONOPS and CRD.
25		PM, OTO	The PM V&V's threat systems and M&S assets, and the OTO accredits them before use in dedicated OT&E. (See **Attachment 17**)
Note: The term OT&E includes IOT&E, FOT&E, MOT&E, QOT&E, FDE, and OUE as defined in AFI 99-103. Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.82 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 DAG AFI 99-103 DASD(AT&L) Memo, *Document Streamlining—Program Protection Plan (PPP)*			

Attachment 23

INTEGRATED TECHNICAL, ENVIRONMENT, SAFETY, AND OCCUPATIONAL HEALTH (ESOH) REVIEWS

Table A23.1. Integrated Technical, Environment, Safety, and Occupational Health (ESOH) Reviews.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	The system is capable of being operated and maintained in its intended operational environment and intended level of maturity with an acceptable level of Environment, Safety and Occupational Health (ESOH) risks. ESOH risks include, but are not limited to: System Safety risks, Human Systems Integration (HSI) risks, and Operational Safety risks.
2		PM	To support all phases of capability maturity, System Safety hazard analysis and other related ESOH documentation are provided to test organizations as they become available to support testing.
3		PM	All system-related ESOH risks have been assessed and accepted at the appropriate management level prior to exposing people, equipment, or the environment to known hazards.
4		PM	Prior to executing any test activities, hazards with a mishap risk level of "Serious" or "High," in accordance with Military Standard (MIL-STD)-882, *DoD Standard Practice System Safety*, are accepted by the appropriate authority as defined in AFI 63-101/20-101.
5		PM	A safety release is provided prior to testing (as necessary). The safety release transmits system ESOH hazard data to the users, maintainers, and testers prior to exposing people, equipment, or the environment to known hazards.
6		PM	Environmental impacts are identified and mitigated or eliminated consistent within cost, schedule, and technical performance considerations. Data about environmental hazards are provided to the test organization to support analyses.
7		PM	All system-related HSI risks are identified and mitigated to the extent possible to minimize illness, disability, death or injury to users, maintainers, and testers.
8		PM	To facilitate the rapid dissemination of System Safety hazard analysis and ESOH documentation between the PM and

			participating test organizations, digital platforms for hosting program safety information (SharePoint, Confluence, Hazard Tracking Systems, etc.) should be used to transmit hazard risks, acceptance, Safety Assessment Reports (SARs), and safety releases.
9		PM	Verified preliminary TOs and technical and/or procedural manuals that identify ESOH risks with mitigation measures are available to support the dedicated OT plan and schedule. (See **Attachment 31**)
10		OTO	User and maintenance personnel have program-specific ESOH training completed in time to support the DT, IT, and OT plans and schedules. (See **Attachment 24**)
11		PM	Appropriate documentation is available from the following sources, when applicable (among others): (1) Non-nuclear Munitions Safety Board; (2) Directed Energy Weapons Safety Board; (3) Flight Safety Board; (4) Airworthiness, Space flight Worthiness; (5) Range Safety; (6) Nuclear Weapons Center; (7) Institutional Review Board for Protection of Human Subjects in Testing; (8) SEEK EAGLE, Obtain operational flight clearances or waivers for systems requiring release or jettison from aircraft (See **Attachment 14**); (9) AF Spectrum Management Office; (10) ATO; (11) CNS/ATM Letter of Compliance
12		OTO	Test organizations independently examine technical and safety risks involving USAF personnel and property prior to test. Utilize all available data to include the Safety Release and technical data provided by the PM. Safety reviews should be accomplished after the technical review so that all test unique hazards are identified and managed in accordance with test design and planned execution. Rapidly acquired capabilities may result in little and/or no prior DT hazard analysis or data to assess OT test hazards; coordinate with the requesting Air Force MAJCOM or USSF Field Command and Mission-Oriented Test Certification Official for risk management and/or additional DT analysis.
13		PM	Systems engineering principles, processes, and practices are properly applied throughout the system life cycle.
14		PM	OT&E plans include V&V of all identified High and Serious ESOH risks and implemented ESOH risk mitigations for all ESOH risks whose initial risk assessment was High or Serious.
Primary References: DoDI 5000.02T, *Operation of the Defense Acquisition System* DoDI 5000.81			

DoDI 5000.85
DoDI 3216.02_AFI 40-402, *Protection of Human Subjects and Adherence to Ethical Standards in Air Force Supported Research*
DAG
MIL-STD-882, *DoD Standard Practice System Safety*
AFI 32-1015, *Integrated Installation Planning*
AFI 62-601, *USAF Airworthiness*
AFI 63-101/20-101
AFI 63-125, *Nuclear Certification Program*
AFI 91-202
AFI 91-204_AFGM2020-01, *Safety Investigation and Hazard Reporting*
AFI 91-205, *Nonnuclear Munitions Safety Board*
AFI 90-801, *Environment, Safety, and Occupational Health Councils*
AFMAN 32-7002, *Environmental Compliance and Pollution Prevention*

Attachment 24

OPERATIONAL TEST TEAM TRAINING

Table A24.1. Operational Test Team Training.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		OTO	Program-specific training requirements and assets for the OT&E test team are identified early and in sufficient detail.
2		OTO	For multi-Service and multi-national systems, any additional training requirements are identified.
3		PM	Any necessary training is adequately contracted for, funded, and scheduled to support the OT&E plan and schedule.
4		OTO	OT&E test team personnel are proficiently trained in T&E procedures and/or operational skills before the start of dedicated OT&E.
5		PM	Training includes normal and abnormal and/or emergency operations to operate and maintain the system(s) according to the LSC and other CONOPS.
6		OTO	User and maintenance personnel are fully trained in Tactics, Techniques, and Procedures, CONOPS, Concept of Employment for System Under Test.
7		OTO	Dry run test procedures before start of dedicated OT&E.
8		OTO	User and maintenance personnel have ESOH training completed in time to support the OT&E plan and schedule.
Primary References: DoDI 5000.75 DoDI 5000.80 DoDI 5000.81 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 DAG AFI 36-2670, *Total Force Development* AFI 99-103			

Attachment 25

SUPPORT EQUIPMENT (SE)

Table A25.1. Support Equipment (SE).

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Peculiar, common, and unique SE are identified as early as feasible.
2		PM	Peculiar SE and its necessary support (e.g., technical data, spares) meets the maintenance times and capabilities stated in the CRD. (See **Attachment 21**, **Attachment 26**)
3		PM	Peculiar SE is available to support the OT&E plan and schedule. Peculiar SE should also be made available to the ITT during DT&E so that any deficiencies can be identified for possible resolution prior to OT&E.
4		PM	Peculiar software SE and its supporting technical data, compilers, manuals, etc., are available if the government maintains the software.
5		PM	Peculiar SE is in production representative configurations and fully interoperable and compatible with the system(s) it supports. (See **Attachment 20**)
6		OTO, PM	Assess any configuration differences between preproduction and production peculiar SE and the expected impact on the validity of dedicated OT&E. (See **Attachment 18**)
7		PM	The government has positive control or oversight over SE configurations. (See **Attachment 18**)
8		User, OTO	Common SE and unique SE are identified and available to support the OT&E plan and schedule.
9		PM	SE training is accomplished or scheduled to support the OT&E plan and schedule. (See **Attachment 23**, **Attachment 29**)
10		PM	Full mission simulators and trainers (e.g., flight simulators) are available at appropriate times and locations for test team training and evaluation in OT&E. Full mission simulators should also be made available to the ITT during DT&E so that any deficiencies can be identified for possible resolution prior to OT&E.
Primary References: DoDI 5000.81			

DoDI 5000.85
DoDI 5000.89
DAG
AFI 99-103
AFI 16-1007, *Management of Air Force Operational Training Systems*
AFI 63-101/20-101

Attachment 26

SUFFICIENCY OF SPARES

Table A26.1. Sufficiency of Spares.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Sufficient spares are available to support test assets, test scenarios, and SE according to the OT&E plan and schedule. This includes sufficient spares to support cybersecurity test activities during DT and OT, with a focus on components targeted for cybersecurity test during the program's MBCRAs (e.g., MRAP-C). Support levels are based on the total number of expected operational test events and hours. Sufficient spares should be made available to the ITT during DT&E so that the schedule can support the entry into OT&E. (See **Attachment 8**)
2		PM	Spares repair procedures and capabilities (for blue suit and/or Contractor Logistics Support) are in place to support the OT&E plan and schedule. (See **Attachment 30**)
3		PM	Provision is made for timely failure confirmation and repair action reports to the OT&E test team. (See **Attachment 30**, **Attachment 31**)
4		PM	The management concepts for primary operating stocks, war readiness spares support, and for battle damage repair are estimated prior to OT&E plan development.
5		PM	Candidate spares for two-level maintenance are identified.
6		User	Spare levels for Mobility Readiness Spares Package and Battle Damage Repair Spares Kit are identified, if appropriate.
7		PM	A logistics support plan is developed and accurately reflects the LSC and other CONOPS. (See **Attachment 8**)
8		PM	Identify the risks and limitations in the spares that support dedicated OT&E. For spares with limited availability, define how quickly they are replenished.
9		PM	The projected number of spares and rates of replenishment supports the ops tempo of the dedicated OT&E.
Primary References: DoDI 5000.81 DoDI 5000.85 AFI 63-101/20-101			

Attachment 27

SUPPORT AGREEMENTS

Table A27.1. Support Agreements.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		OTO	Memorandums of Understanding (MOU) and Memorandums of Agreement (MOA) should establish the availability of test and support resources needed for the OT&E plan and schedule.
2		OTO	For a MOT&E, comply with the terms of the *Memorandum of Agreement on Multi-Service Operational Test and Evaluation (MOT&E) and Operational Suitability Terminology and Definitions*, for guidance on conduct, execution, and reporting. A copy of the MOT&E MOA is available by email if a request is sent to: AFOTEC.A5A8.Workflow@us.af.mil.
3		OTO	Interagency support agreements should be established for using ranges, test facilities, airspace, frequencies, etc., and base support functions such as supply, transportation, and billeting.
4		OTO	Support agreements should be established with other government agencies for such functions as data processing, failure analysis, communications, and security.
5		ITT	Obtain agreements for testing interoperability, cybersecurity, cyber resiliency, network risk assessments, etc. (See **Attachment 9**, **Attachment 10**, **Attachment 13**)
6		OTO	The potential for conflict of interest is strictly avoided, mitigated, or neutralized before any contractor is allowed to participate in the support of dedicated OT&E. (See **Attachment 30**)
Primary References: DoDI 4000.19, *Support Agreements* AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*			

Attachment 28

PACKAGING, HANDLING, STORAGE & TRANSPORTATION

Table A28.1. Packaging, Handling, Storage & Transportation.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	Shipping containers, packaging, handling, storage, and transportation components and methods are fully qualified and meet the CRD's requirements.
2		PM	Operationally relevant maintenance demonstrations and scenarios are used as specified in the LCSP.
3		PM	Adequate numbers of production representative shipping containers, packaging, handling, and transportation vehicles are used to transport test articles to the dedicated OT&E sites.
4		PM	Formal or preliminary technical data are verified and available to support the dedicated OT&E plan and schedule. (See **Attachment 31**)
5		OTO	Shipping, transportation, receiving, and storage arrangements are in place with the contractor and host base transportation offices for accountability and timely shipping, receiving, and resource protection of test and support assets.
6		PM	OT&E test team maintenance personnel are adequately trained. (See **Attachment 24**)
7		PM	Proper security protocols for packaging, handling, storage and transportation for classified systems are followed.
Primary References: DoD Manual 4140.01 V2, V7 AFI 63-101/20-101			

Attachment 29

PERSONNEL

Table A29.1. Personnel.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		OTO	Identify OTO test team personnel requirements, including software maintenance skills, certifications and security clearances. The number of personnel and skill levels reflects typical operational users in the operational environment.
2		OTO	Written agreements are in place establishing the sources for necessary personnel. (See **Attachment 11**, **Attachment 28**)
3		PM	Estimates of maintenance requirements (in terms of man hours and personnel) for line-replaceable units, subsystems, and the full system are available. (See **Attachment 8**, **Attachment 25**)
4		PM	Contractor support provided by the system contractor during OT&E is consistent with planned operational contractor support in accordance with DoDI 3020.41, *Operational Contract Support (OCS)*. (See **Attachment 30**)
5		PM	Necessary training, including Type 1 and/or Type 4 training, are completed or scheduled for completion to support the dedicated OT&E plan and schedule. (See **Attachment 24**)
Primary References: DoDI 5000.75 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 DAG			

Attachment 30

CONTRACTOR SUPPORT

Table A30.1. Contractor Support.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		OTO	All contractor assistance or services (to include participation in or support to mishap investigations) necessary to support dedicated OT&E are identified in the OT&E test plan, TEMP, Request for Proposal, Performance Work Statements, and Statement of Work.
2		OTO	The potential for conflict of interest is strictly avoided, mitigated, or neutralized before any system contractor is allowed to participate in the support of dedicated OT&E. Contact the Contracting Officer prior to allowing a system contractor to participate in the support of dedicated OT&E.
3		OTO	OSD approval is obtained for the following types of system contractor involvement in dedicated OT&E. Care is taken to minimize conflicts of interest when the system contractor is involved in dedicated OT&E.
4		OTO	Contractor maintenance and support actions may be conducted by the system contractor if it is also planned for the system contractor to provide Interim Contractor Support or Contractor Logistics Support after the system is deployed.
5		OTO	System contractor should conduct and report failure analyses to assist in isolating causes of test failures.
6		OTO	System contractor should provision system-unique test equipment, test beds, test facilities, instrumentation, data collection, and analysis.
7		OTO	System contractor should provide logistics support and training (Type 1) if such services have not yet been developed and are not available from government sources.
8		PM	If the system contractor is approved to conduct ILS or Contractor Logistics Support, they established report generation procedures and deliver reports for depot-level repair and maintenance actions. (See **Attachment 13**, **Attachment 19**)
9		OTO	Coordination with the program office has been done to establish support contractor services for any data collection, reduction, and analysis capabilities needed throughout testing not performed by

			the government. (See **Attachment 10**, **Attachment 11**, **Attachment 22**, **Attachment 27**)
Primary References: 10 USC §2399, *Operational Test and Evaluation of Defense Acquisition Programs* DoDI 5000.75 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 AFI 99-103 AFI 25-201 *Incorporating Test and Evaluation into Department of Defense Acquisition Contracts*			

Attachment 31

TECHNICAL DATA

Table A31.1. Technical Data.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	User and maintainer technical data (e.g., TOs, engineering drawings, specifications, standards, updated Department of Defense Architecture Framework system views, process and user manuals, technical reports, catalog items) are available to support the OT&E plan and schedule. Technical data should be made available to the ITT during DT&E so that any deficiencies can be identified for possible resolution prior to OT&E.
2		PM	All technical data are managed according to a Configuration and Data Management Plan. (See **Attachment 18**)
3		User	Technical data from other interoperable systems are available to support the OT&E plan. (See **Attachment 11**)
4		PM	Technical data for evaluating system suitability and software supportability are available.
5		User	Sufficient information is provided for successfully operating and maintaining the system.
6		PM	Formal or verified preliminary TOs and technical data are available for use in dedicated OT&E.
7		PM	A Technical Order Management Agency is in place to manage TO deliveries, changes, and other TO requirements.
8		PM	Procedures are established to process changes to technical data and TOs.
Primary References: DoDI 5000.75 DoDI 5000.81 DoDI 5000.85 DoDI 5000.87 DAG TO 00-5-1, *Air Force Technical Order System* TO 00-5-3, *Air Force Technical Order Life Cycle Management*			

Attachment 32

TEST & EVALUATION RESOURCES

Table A32.1. Test & Evaluation Resources.

Note: Check the following actions have been taken if applicable. Recommended OPR(s) indicated below.			
#	Done	OPR	Action
1		PM	T&E infrastructure shortfalls are identified in draft and current versions of the TEMP. HQ USAF/TE is informed of shortfalls.
2		OTO	Sufficient resources and funding are available to start and sustain the planned OT&E program.
3		OTO	Test ranges and facilities are properly equipped, manned, funded, scheduled, and personnel briefed before start of dedicated OT&E.
4		PM	Cybersecurity test infrastructure (with appropriate architecture, level of realism, and security), and resources to conduct cyber vulnerability and penetration assessments and adversarial assessments, and documentation are available and described in the TEMP. (See **Attachment 12**)
5		PM	Realistic targets (or V&V'd simulators) are in the most current operational configuration(s) and available in sufficient quantities. (See **Attachment 17**, **Attachment 18**)
6		OTO	Test threat systems and related support, including countermeasures, are identified and programmed as early as possible.
7		OTO	Sufficient threat densities, either in open-air or indoor facilities, rigorously stress the system in as realistic a combat environment as possible. (See **Attachment 16**)
8		OTO	Validated cyberspace threats are emulated and/or employed to the extent possible to create a cyber-contested environment during adversarial penetration and exploitation testing.
9		OTO	Adequate test instrumentation and data reduction capabilities are identified, funded, scheduled, and support agreements negotiated on utilization rates and data requirements.
10		OTO	M&S assets (including simulators, test drivers, and scenarios) are accredited, scheduled, and available to support the DT&E and OT&E plans and schedules.
11		PM	An environmental impact study or assessment (if required) addressing federal, state, DAF, and local regulations are

			completed and approved or waivers granted. (See **Attachment 23**)
12		OTO	Other interoperable systems and subsystems test articles, including external systems are available. (See **Attachment 9**)
Primary References: DoDI 5000.75 DoDI 5000.85 DoDI 5000.87 DoDI 5000.89 DoD 7000.14-R, *Department of Defense Financial Management Regulations,* Vol 2A DAG DoD Cybersecurity T&E Guidebook AFI 65-601, *Budget Guidance and Procedures,* Chapter 14 AFI 99-103			