Test and Evaluation Guidebook

Revision 6

August 27, 2024

APPROVAL:

THOMAS A TOMAIKO

Digitally signed by THOMAS A TOMAIKO
Date: 2024.09.03 18:30:40 -04'00'

_____

Thomas Tomaiko
Independent Test Agent
Executive Director, Test and Evaluation Division
Acquisition Program Management
Transportation Security Administration

TABLE OF CONTENTS

SECTION NO. PAGE NO.

1.0 PURPOSE 1

1.1 T&E OVERVIEW 2

1.2 T&E PRINCIPLES 2

1.3 T&E ORGANIZATION 3

1.4 ACQUISITION PROGRAM CATEGORIES 5

1.5 T&E METRICS AND INFORMATION SHARING 5

2.0 T&E ROLES AND RESPONSIBILITIES 6

2.1 SYSTEM EVALUATOR 6

2.2 OPERATIONAL TEST DIRECTOR 7

2.3 T&E MANAGER 9

2.4 QUALIFICATION TEST DIRECTOR 10

2.5 DESIGNATED GOVERNMENT CERTIFICATION AGENT 11

2.6 T&E STAKEHOLDER ORGANIZATIONS 11

2.6.1 APM/PEO 12

2.6.2 APM/Capability and Acceptance Management Branch 12

2.6.3 APM/Deployment and Sustainment Division 12

2.6.4 CAE Staff 12

2.6.5 Contracting and Procurement 12

2.6.6 IT/IAD 12

2.6.7 IT/Governance, Risk, and Compliance 13

2.6.8 Intelligence and Analysis 13

2.6.9 Occupational Safety, Health, and Environment 13

2.6.10 Requirements and Capabilities Analysis/Analysis and Engineering 13

2.6.11 RCA/Capabilities Management and Innovation 13

2.6.12 Training and Development 14

3.0 T&E STRATEGY AND PLANNING 15

3.1 T&E IPT 15

3.2 SYSTEM EVALUATION TEAM 16

3.3 REVIEWING AND ASSESSING REQUIREMENTS 16

3.4 USE OF THIRD PARTY TESTING IN A SYSTEM EVALUATION 16
3.5 DEVELOPING EVALUATION CRITERIA 17
3.6 TES DEVELOPMENT 18
3.7 TEMP DEVELOPMENT 19
3.7.1 Evaluation Framework 20
3.7.2 Modeling and Simulation 21
3.8 SYSTEM EVALUATION PLAN 22
3.9 TEST AND EVALUATION CONCEPT BRIEFING 22
3.10 DETERMINING THE SCOPE OF TESTING AFTER A SYSTEM CHANGE 22
4.0 DEVELOPMENTAL, CERTIFICATION, AND QUALIFICATION TESTING ... 25
4.1 TEST EVENT OVERVIEW 26
4.2 QT PLANNING 28
4.2.1 Planning Documentation 29
4.2.2 Coordination of System Delivery and Installation 29
4.2.3 Establishing the Configuration Baseline Prior to Qualification Testing 29
4.2.4 Test Readiness Notification 30
4.2.5 Threat Items for CERT 31
4.2.6 Test Article Selection and Development 31
4.2.7 Test Tool Development and VV&A 31
4.2.8 Coordination with Supporting Organizations 32
4.2.9 QT Readiness Review 33
4.3 QT EXECUTION AND REPORTING 33
4.3.1 Test Execution 34
4.3.2 QT DAG 34
4.3.3 Data Analysis and Reporting 35
4.3.4 Results Adjudication 36
4.3.5 Regression QT 37
4.3.6 Test Article Management 38
4.3.7 Configuration Control During Test Execution 38
4.3.8 Maintenance Activities 39
4.3.9 Termination of QT Activities 39

5.0 OPERATIONAL TESTING 40
5.1 OT EVENTS OVERVIEW 40
5.2 OT PLANNING 41
5.2.1 Operational Test Plan 42
5.2.2 OA Plan and OUE Plan 42
5.2.3 Site Selection 43
5.2.4 Test Site Coordination and In-Briefs 45
5.2.5 Establishing Baseline Capability 46
5.2.6 Test Team Preparation and Training 46
5.2.7 OT TRN 46
5.2.8 Verifying the System Configuration Prior to Test Execution 47
5.2.9 Configuration Control During Test Execution 48
5.2.10 Operational Test Readiness Review 48
5.3 BURN-IN AND TEST EXECUTION 50
5.3.1 Burn-In 51
5.3.2 Test Execution and Data Collection 51
5.3.3 Early Termination of Operational Testing 51
5.3.4 Test Closeout and Site Restoration 52
5.4 TI TESTING 52
5.4.1 TI Test Planning 52
5.4.2 TI Execution 53
5.4.3 Working with TI Data 53
5.4.4 Test Article Security 54
5.5 OT DATA AUTHENTICATION 54
5.5.1 OT DAG Personnel 54
5.5.2 DAG Scoring Criteria 55
5.5.3 DAG Procedures 55
5.6 OT EVENT REPORTING 56
5.6.1 OT QLR 56
5.6.2 OT ERB 56
5.6.3 OA Report 56

5.6.4 OUE Report 57
6.0 SYSTEM EVALUATION REPORT 58
6.1.1 Test Event Reporting in Support of the SER 58
6.1.2 SER Development 58
6.1.3 SER Review and Approval 59
6.1.4 SER Redress Memorandum 60
7.0 ACCEPTANCE TESTING 61
7.1 ACCEPTANCE TESTING 61
7.1.1 First Article Test and Evaluation 65
7.1.2 Factory Acceptance Test 65
7.1.3 SAT and ORT 66
7.1.4 AT Reporting 68
7.2 INTEGRATION ACCEPTANCE TESTING 70
7.2.1 Network Throughput Test 71
7.2.2 Integrated System Acceptance Test 72
7.2.3 Operational Run-in & Closeout 78
7.2.4 ISAT and Operational Run-in Data Analysis 78
7.2.5 Integration Testing Reporting 79
7.3 BAGGAGE ASSESSMENT AND SYSTEM EVALUATION 80
7.3.1 CBIS PGDS 81
7.3.2 BHS CBIS Support 81
7.3.3 CBIS Design Reviews 81
7.3.4 BASE Efforts 82
7.3.5 CBIS R&D 82
7.4 LABORATORY/FACILITY BHS SUPPORT 83
7.4.1 TSIF BHS 83
7.4.2 TSALC BHS Loop 83
7.5 ACCEPTANCE TESTING AND SYSTEM ASSESSMENT TEST ARTICLES 83
7.5.1 Image Quality Test Kits 83
7.5.2 SOC Representative Test Articles 84
7.5.3 ISAT Test Articles 84

7.5.4 Donations: ATSA Logistical Support 84

APPENDIX A: ACRONYM LIST A-1

APPENDIX B: TEST AND EVALUATION PLANS, REPORTS, AND OTHER SUPPORTING DOCUMENTATION B-1

APPENDIX C: REFERENCES C-1

APPENDIX D: CYBERSECURITY EVALUATION GUIDANCE D-1

APPENDIX E: DOCUMENTATION GUIDELINES E-1

APPENDIX F: TEST AND EVALUATION ROLES AND RESPONSIBILITIES F-1

LIST OF TABLES

TABLE NO. **PAGE NO.**

Table 3-1: Change Package Tier Designations 24
Table 4-1: Developmental / QT Events 27
Table 4-2: QT DAG Personnel 35
Table 4-3: Determination of Compliance with Requirements 36
Table 4-4: QT Severity Ratings (Adjudicated) 37
Table 5-1: Operational Testing Activities 40
Table 5-2: OT DAG Personnel 54
Table 7-1: Types of ATs 62
Table 7-2: Types of Integration ATs 70

LIST OF FIGURES

FIGURE NO. **PAGE NO.**

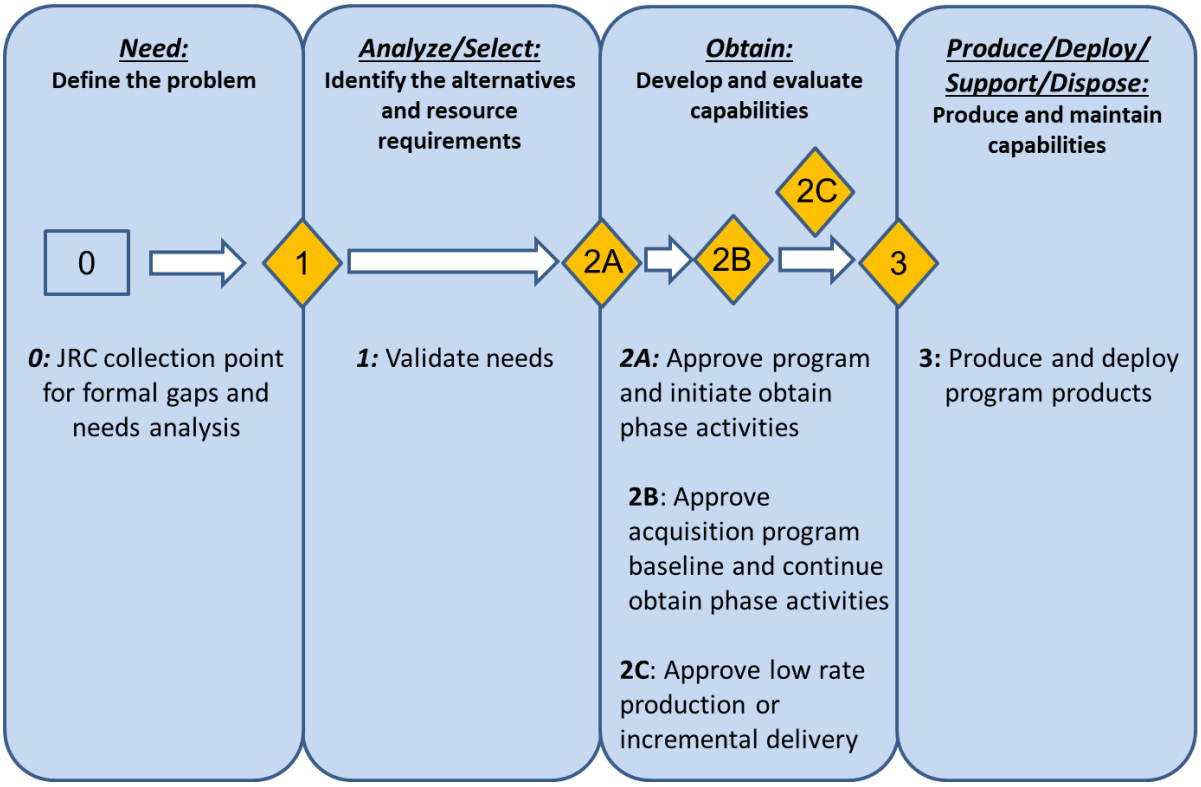
Figure 1-1: Acquisition Lifecycle Framework 1
Figure 3-1: TES and Evaluation Planning Process Flow 15
Figure 3-2: ITA Review of External Data 17
Figure 3-3: Example Criteria and Derived Measures 18
Figure 3-4: Relationship of COIs, Criteria, and Measures 19
Figure 3-5: TEMP to Reporting Hierarchy 20
Figure 3-6: Changes to Deployed Systems Process 23
Figure 4-1: Qualification Test Planning Process Flow 28
Figure 4-2: QT Execution Process Flow 34
Figure 5-1: OT Planning Process Flow 41
Figure 5-2: Site Selection Process 43
Figure 5-3: OT Execution Process Flow 50
Figure 6-1: Evaluation Reporting Process Flow 58
Figure 7-1: AT Process 64
Figure 7-2: ISAT Process 74

1.0 PURPOSE

The Transportation Security Administration (TSA) Test and Evaluation (T&E) Guidebook describes how TSA T&E organizations, in collaboration with stakeholders, plan and execute an effective and efficient T&E Strategy (TES). The guidebook aligns with the *TSA T&E Management Directive (MD) 2600.4*, dated August 21, 2024, and meets the spirit and intent of overarching Department of Homeland Security (DHS) policy as described in the *Department of Homeland Security (DHS) Acquisition Management Directive 102-01,* dated February 25, 2019, and *DHS Directive 026-06, Test and Evaluation*, dated October 01, 2020. Additionally, this guidebook aligns with the *TSA Acquisition Manual (TSAAM),* dated June 2023.

The T&E activities described in this guidebook support the DHS Acquisition Life Cycle Framework (ALF). The ALF, depicted in **Figure 1-1**, identifies the four phases required for system acquisition at DHS and the associated Acquisition Decision Events (ADEs).

Figure 1-1: Acquisition Lifecycle Framework



A successful ADE reflects approval to continue to the next ALF phase as well as the commitment of effort and funds. T&E provides evaluation results and conclusions to inform decision makers during the Acquisition Review Board (ARB) meeting that assists the Acquisition Decision Authority (ADA) in determining whether to proceed to the next phase of the acquisition life cycle.

1.1 T&E Overview

TSA/Acquisition Program Management (APM) performs T&E to determine whether a system, inclusive of technology, operator, and procedures, meets operational and functional requirements. TSA T&E organizations support the T&E of a wide variety of systems from checked baggage and passenger screening Transportation Security Equipment (TSE) to Information Technology (IT) systems. This revision of the guidebook focuses on the T&E procedures for the assessment of TSE.

Acquisition Management Directive 102-01 applies to Acquisition Level 1 and Level 2 programs and programs designated as special interest by the Undersecretary of Management. TSA T&E organizations may also assess capabilities not directly associated with an acquisition program (e.g., technology demonstration of emerging capability). This guidebook is primarily focused on the T&E processes associated with acquisition programs. The guidebook clearly identifies any explanation of processes not associated with acquisition program T&E when presented.

Throughout this guidebook, there are recurring references to Operational Effectiveness, Suitability, and Resilience. These terms are critical to the overall goals and outcomes of T&E and defined as follows:

- *Operational Effectiveness* is the overall ability of a system to accomplish mission objectives when used by representative personnel in the environment expected for operational employment considering organization, procedures, supportability, vulnerability, and threat.
- *Operational Suitability* is the overall degree to which a system can be satisfactorily used with consideration given to transportability, interoperability, reliability, maintainability, availability, safety, human-systems integration, manpower, logistics supportability, and training requirements.
- *Operational Resilience* is the overall ability of the system to protect, detect, counter react to threats, and restore capabilities, to include exploitation potential and mission impact. A critical component/criterion of operational resilience is cyber resilience. Cyber resilience is an assessment of the system's ability to remain effective and suitable to satisfy the mission while under duress from offensive cybersecurity attack.

1.2 T&E Principles

TSA Test Teams conduct T&E following a set of four T&E principles. These principles enable T&E Teams to support the material objectives of speed to field and increased performance by discovering problems early using efficient and proven T&E methods. The four T&E principles are:

- Early Test Involvement
- Tailor to the Situation
- Integrated and Parallel Testing
- Streamline Processes and Products

In support of early test involvement, TSA T&E Teams conduct Operational Utility Evaluations (OUEs) in the field and/or Data Collection Activities in laboratory environments in support of Research and Development (R&D) activities, such as in support of the Innovation Task Force (ITF). These events allow for the early identification of system capabilities and limitations to assist vendors in their system design and development. The events also assist TSA in deciding whether a system is of a sufficient level of maturity to proceed through the acquisition/qualification process.

T&E tailors its early T&E support to the event sponsor's needs, ensuring the T&E Team collects and provides the precise sought after data in an expeditious manner. To accomplish these goals, T&E typically develops a concise, incremental, test plan (e.g., OUE Plan) and report (e.g., OUE Report). T&E Teams will help sponsors develop data collection strategies and approaches when documented requirements are not available.

Further tailoring may occur in support of acquisition programs when the Independent Test Agent (ITA) conducts Operational Assessments (OAs) to assess overall readiness to proceed to an Operational Test (OT). If documented in the approved Test and Evaluation Master Plan (TEMP), the ITA may streamline the OT event by utilizing data from the OA as a primary system evaluation data source.

When planning for a test event, the ITA is responsible for assigning a primary test entity to verify individual test measures (and requirements). During this activity, the ITA should pursue methods to increase test execution efficiency such as pursuing an integrated test event if feasible and/or parallel execution of test activities. Integrated testing is the collaborative planning and execution of test phases and events to provide data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the Qualification Test (QT), and OT entities. The ITA attempts to minimize the sequential/serial execution of test events as it delays acquisition and fielding timelines.

1.3 T&E Organization

The TSA Executive Director of the APM/T&E Division (hereafter referred to as the Executive Director, ITA) leads the TSA ITA. The ITA performs the independent evaluation of Operational Effectiveness, Suitability, and Resilience and is comprised of the APM/T&E Division as approved by the Director, Office of Test and Evaluation (DOT&E). The APM/T&E Division consists of the branches listed below.

- The System Evaluation Branch (SEB) is responsible for the overall evaluation of the Operational Effectiveness, Suitability, and Resilience of a system. The SEB produces OUE Reports in support of R&D efforts and System Evaluation Reports (SERs) in support of acquisition decisions.
- The Operational Test Branch (OTB) plans and conducts OAs and OTs in support of the SEB overall system evaluation. The OTB also plans and conducts OUEs in support of R&D efforts.

- The TSA Systems Integration Facility (TSIF) Test Branch (TTB) plans and conducts QT events at the TSIF to verify system technical capability in support of the overall system evaluation. The TTB generally verifies non-detection-related functional requirements, however, they may verify detection-related requirements when needed. The TTB also serves as the Designated Government Certification Agent (DGCA), or in a supporting role to the DGCA, for non-explosives detection and false alarm verification (e.g., Prohibited Item [PI] detection). The TTB also supports Data Collection Activities in support of R&D efforts.
- The Test Infrastructure and Operations Branch (TIOB) supports TTB and OTB test activities by providing facility, test article, Configuration Management (CM), and other related logistical and infrastructure support.
- The Acceptance Test and System Assessment (ATSA) Branch (hereafter referred to as ATSA) is responsible for providing Acceptance Test (AT) support activities for T&E events and in support of deployment activities post-ADE-3.

The following entities provide data to the ITA evaluation of candidate systems as a DGCA, or in support of the DGCA, as documented in the program TEMP. Additional information concerning the role of the DGCA can be found in the *TSA Transportation Security Equipment Certification Policy,* dated April 21, 2021. As such, the APM/T&E Division includes functional leadership who coordinate directly with these entities:

- The DHS/Science and Technology/Transportation Security Laboratory (TSL)/Independent Test and Evaluation (IT&E) Division conducts Certification Testing (CERT) in the areas of explosives detection and false alarm verification against approved detection standards. TSL/IT&E also supports ad-hoc special studies and exploratory testing on an as needed basis. The System Evaluator typically uses the CERT as a primary input to the Operational Effectiveness determination. The TSL/Developmental Test and Evaluation Division supports the development of candidate technologies by providing Certification Readiness Assistance and Readiness Testing prior to formal CERT and supporting ad-hoc special studies as needed. The TSL Deputy Director is functionally aligned within the APM/T&E Division.
- The Federal Bureau of Investigation's (FBI's) Terrorist Explosive Device Analytical Center (TEDAC) Improvised Explosives Detection and Synthesis (TIEDS) Center supports FBI, Science and Technology, and TSA's Research, Development, Test, and Evaluation priorities to assess the safety and performance characteristics of improvised explosives and assess performance of detection technologies against existing and emerging threats. In this regard, the TSL and TIEDS operate in tandem to assess TSA system performance against explosives detection requirements. The TIEDS Center is comprised of an explosive synthesis and testing laboratory, a trace explosives laboratory, the detection technology center, and explosives testing range. The TIEDS TSA onsite infrastructure lead is functionally aligned within the APM/T&E Division.

The ITA may leverage data from other data sources both internal to TSA (e.g., IT/Information Assurance and Cybersecurity Division [IAD]) and external to TSA (e.g., third party test organizations) in its evaluation under certain conditions. Stakeholder organizations are

documented in section 2.6. One can find additional details on the ITA's use of external data sources in the *Third Party Testing Framework,* dated October 04, 2021, and in section 3.4 of this guidebook.

1.4 Acquisition Program Categories

Throughout this guidebook, there are references to acquisition programs in four categories as defined below.

- Major Programs (Non-Delegated Systems): Any system within a major program as designated in the DHS Master Acquisition Oversight List (MAOL) in a non-delegated status. These generally consist of systems within Level 1 and Level 2 programs that have not received an initial successful ADE-3 decision. The ADA for major programs (non-delegated systems) is the DHS Chief Acquisition Officer.
- Major Programs (Delegated Systems): Any system within a major program, as designated in the DHS MAOL in a delegated status. These generally consist of systems within Level 1 and Level 2 programs that have received a successful ADE-3 fielding decision with delegation status formally granted by the Chief Acquisition Officer at the ADE-3 and documented in the associated Acquisition Decision Memorandum (ADM). The ADA for major programs (delegated systems) is the Component Acquisition Executive (CAE).
- Major Program (Post-Full Operational Capability [FOC] Delivery): A major program designated as post-FOC delivery in the DHS MAOL. These programs generally differ from those previously described in that all systems within these programs are in the acquisition sustainment / operations and maintenance phase. The ADA for major programs (post-FOC delivery) is the CAE.
- Non-Major Programs: Programs designated as "non-major" in the DHS MAOL. These generally consist of Level 3 programs. The ADA for non-major programs is the CAE.

This guidebook denotes any differences in the planning, execution, and reporting based on program categorization in the appropriate sections.

1.5 T&E Metrics and Information Sharing

The T&E Division test branches are responsible for the ongoing tracking and reporting of T&E activities to include test events planned and completed, plans and reports delivered, and event tracking against program-defined milestones. This tracking feeds a division dashboard that is utilized to compile accomplishments for end-of-year reporting and to understand potential deficient areas and improvement opportunities.

The T&E Division also requires its test branches to maintain an easily accessed repository for maintaining and sharing T&E policy and procedure, templates, signed plans and reports, and tracking mechanisms for T&E Division-provided T&E recommendations and for any ADM action items assigned to the T&E Division. As such, the test branches have processes in place for ensuring these repositories are current and documents are easily accessed (e.g., intuitive folder structure, standard naming convention) to allow for easy reference and effective sharing across the division.

2.0 T&E ROLES AND RESPONSIBILITIES

The primary functional roles responsible for T&E at TSA are listed in overarching documentation, specifically, the DHS Acquisition Management Directive 102-01, DHS Management Directive 026-06, the TSA T&E Management Directive 2600.4, and the TSA Transportation Security Equipment Certification Policy.

The roles critical to support the execution of T&E at TSA are the T&E Manager, System Evaluator, Operational Test Director (OTD), QT Director (QTD), and the DGCA. The following sections describe the responsibilities for these critical roles.

2.1 System Evaluator

The System Evaluator is a member of the ITA and responsible for leading the evaluation of Operational Effectiveness, Suitability, and Resilience. Specifically, the System Evaluator:

(1) Leads the System Evaluation Team (SET) and ensures the SET activities are in accordance with the program TEMP, T&E Policy, and T&E guidelines. Ensures coordination across all T&E stakeholders on subject matter that supports the system evaluation.

(2) Reviews all requirements to ensure that they are testable, measurable, and achievable.

(3) Works with the T&E Manager and the OTD to determine the TES and the test activities required to evaluate a system to support the acquisition strategy identified by the Program Management Office (PMO). Briefs the TES to the Executive Director, ITA in the form of an Early Strategy Review (ESR). The Executive Director, Program Execution Office (PEO) should also attend the ESR for major programs (non-delegated systems).

(4) Collaborates with the T&E Manager to develop the Evaluation Framework (EF).

(5) Provides the TES inputs in the TEMP.

(6) Provides input to the TES briefing. As requested by the PMO, leads the presentation of the T&E approach in the TES briefing.

(7) For deployed systems, develops a Determination of Test Scope (DTS) for Tier 3-proposed system changes as further defined in section 3.8.

(8) Develops the System Evaluation Plan (SEP).

(9) Develops the Test and Evaluation Concept Briefing (TECB). Presents the TECB to DOT&E.

(10) Leads the threat working group to define the threat/threat set required to support Certification test efforts for the program's detection requirements. In collaboration with the T&E Manager and DGCA, facilitates the endorsement or approval of the threat sets.

(11) Authors the threat validation memorandum for Threat Inject (TI) test articles.

(12) Reviews and concurs with all test plans to ensure the test and data collection methodologies are adequate to support the evaluation plan/strategy.

(13) Responsible for the final selection of OT sites using input from the OTD and the SET.

(14) Chairs Data Authentication Group (DAG) meetings, Reliability, Maintainability, Availability (RMA) scoring conferences (if held separately from the DAG), and Adversarial Assessment (AA) vulnerability scoring conferences with support from the OTD. Considers all inputs from DAG members and provides the final authentication decision for test data.

(15) Issues a CERT Letter Concurrence memorandum to the PMO prior to PMO issuance of a vendor Certification Letter.

(16) Authors the OT Quick Look Report (QLR), SER (and corresponding TI Report if required), OA Report, and OUE Report. Drafts a SER Communication Memorandum (SCM) and works with the APM Front Office to communicate the SER to stakeholder organizations. Archives all final approved reports in the OTB/SEB document library.

(17) Reviews and provides feedback to the DOT&E-developed Letter of Assessment (LOA).

(18) Upon PMO request, supports the development of program/acquisition materials that contain T&E results. Upon request, supports the program's presentation of these results to leadership at Acquisition Review Team meetings and ARB meetings.

(19) Upon PMO request, supports Technical Interchange Meetings (TIMs) with vendors where the results of T&E are discussed.

2.2 Operational Test Director

The OTD is a member of the ITA and is responsible for leading the planning and execution of OA and OT activities. Specifically, the OTD:

(1) During TES Development and Evaluation Planning:

a. Reviews all operational requirements to ensure that they are operationally meaningful, testable, measurable, and achievable and ensures the OT design is adequate to address requirements.

b. Communicates required OT level of effort (e.g., sites, duration, test staff) with ITA leadership and stakeholders to ensure appropriate resources are available for a timely OT start.

c. Provides input as requested by the PMO or the T&E Manager for the PMO-managed Integrated Master Schedule (IMS) concerning test activity timelines.

d. Provides OT inputs to the TEMP, as requested by the T&E Manager, and SEP.

e. Supports the T&E Manager and System Evaluator by providing input to EF development with a focus on the OT data source assignments for requirements.

f. Provides input to the ESR briefing and TECB, and presents OT portions in coordination with the System Evaluator. Coordinates with the T&E Manager and PMO during the development of the TES and presents the OT portions of the TES briefing as needed.

g. Coordinates the development of threat articles with the SET and coordinates test article approvals for testing as needed.

(2) During OT/OA/OUE Planning:

a. Leads the site selection process to include coordination with the user organization and deployment stakeholders, and conducting site surveys as required, to understand site usage of relevant systems and provides a list of recommended sites to the System Evaluator for final selection.

b. Develops the Operational Test Plan (OTP) and OA Plan to include AA planning and all other required test and data methodologies in alignment with the evaluation strategy/plan. Develops OUE Plans in support of R&D efforts. Archives all final approved plans in the OTB/SEB document library.

c. Reviews and approves all data collection forms, ensuring they are suitable to capture the required data elements from the test plan.

d. Develops the TI testing design of experiments and conducts TI test article validation at the TSIF when necessary.

e. Works with the support contractor to ensure resources are identified, properly trained, and available to start testing per approved timelines.

f. Conducts airport Federal Security Director (FSD) briefs and periodic coordination calls with local TSA to ensure test site readiness according to schedules.

g. Coordinates the completion of all required entrance criteria, ensuring a timely start to OT, OA, or OUE activity. Leads the Operational Test Readiness Review (OTRR) criteria tracking during the SET. Presents the OTRR to leadership.

(3) During OT/OA/OUE execution:

a. Leads the test execution and coordination of site activities.

b. Delivers the Start of Testing Notification (STN) upon completion of burn-in. Alternatively, suggests extension of burn-in or escalates other issues as appropriate.

c. Monitors test progress against the test plan and delivers daily status reports to the SET. This requires working closely with the support contractor analyst to ensure the T&E Team is collecting data according to the test plan with an understanding of sample sizes collected to date, target sample size, and test duration remaining.

d. Escalates issues, as appropriate, to include test extension or termination recommendations.

e. Leads the presentation of data at the DAG, RMA scoring conference, and AA vulnerability scoring conference, and provides input on the scoring of data, to include any Test Incident Reports (TIRs).

(4) During OT/OA/OUE reporting:

a. Reviews and provides the System Evaluator with the dataset as authenticated in the DAG sessions.

b. Develops the Emerging Results Briefing (ERB) for OT events under DOT&E oversight.

c. Supports classified TI DAG sessions and reviews the TI Report.

d. Reviews and concurs with the OT QLR, OA Report, OUE Report, SER, and/or any other reporting artifact or memorandum.

e. Reviews and provides feedback to the DOT&E-developed LOA.

f. Upon PMO request, works with the System Evaluator to develop program/acquisition materials that contain the results of the OT/OA/OUE. Upon request, supports the program's presentation of these results to leadership.

g. Upon PMO request, supports TIMs with vendors in which discussion of T&E results occur.

2.3 T&E Manager

While the T&E Manager is functionally aligned within the APM/T&E Division, they are not a representative of the ITA. In accordance with *DHS Test and Evaluation Instruction 026-06-001*, the T&E Manager acts as the focal point for T&E efforts. Specifically, the T&E Manager:

(1) Supports the Program Manager (PM) by providing TES and risk mitigation input during the development of an Acquisition Strategy.

(2) Coordinates T&E activities by providing insights to stakeholders concerning TES, T&E processes, T&E guidelines, planning, execution and reporting documentation, as well as the relationship to Capability Manager- and acquisition-related documentation required to support T&E efforts.

(3) Provides input to the PMO to support technically informed and objective judgement on T&E planning, execution, and reporting. Assists in the planning and coordination of resources to support the program's T&E efforts.

(4) Schedules and facilitates discussions between PMO, T&E Division, TSL, and other stakeholders upon request to mitigate T&E issues due to schedule or resources conflicts or to address stakeholder requests for accelerated or other unique test services, as needed and upon request.

(5) Provides input to the program IMS, and tracks and communicates the T&E schedules for assigned acquisition programs. Coordinates with the PMO and the ITA to mitigate issues that result in a shift right to the schedule.

(6) Provides input into all requirements to ensure that they are testable, measurable, and achievable. Coordinates Functional Requirements Document (FRD) review with the ITA and ensures the PMO reviews and adjudicates ITA feedback.

(7) Chairs the T&E Integrated Product Team (IPT) as delegated by the PM.

(8) Collaborates with the System Evaluator to determine the TES and the test activities required to evaluate a system to support the PMO acquisition strategy.

(9) Provides input into the System Evaluator's ESR briefing to the Executive Director, ITA.

(10) In support of the PM and in coordination with the ITA, develops the TEMP and TES briefing. Supports the PM and ITA in briefing the TES to DOT&E as needed.

(11) With the System Evaluator, develops the EF.

(12) Reviews and provides feedback on test briefings, plans, and reports such as the SEP, TECB, OTP, and SER to ensure alignment with the TEMP.

(13) Participates in and provides feedback at DAG meetings.

(14) Reviews and provides feedback to the DOT&E-developed LOA.

(15) Supports the PM in the development of program/acquisition materials that contain T&E results. Upon request, supports the program's presentation of these results to leadership at ART meetings and ARBs.

(16) Upon PMO request, supports TIMs with vendors in which discussion of T&E results occur.

(17) Supports the DGCAs in the development and revision of the Certification Test Management Plans as per TSA CERT policy for PM signature.

(18) Reviews and provides input to the System Evaluator concerning the T&E Division Memorandums: (DTS, SCM, CERT Letter Concurrence memorandum).

(19) Supports the program procurement documents (e.g., Request for Proposals) to ensure T&E equities have been included.

2.4 Qualification Test Director

The QTD is a member of the ITA and is responsible for leading the planning, execution and reporting of QT activities. Specifically, the QTD:

1) Reviews all technical and functional requirements to ensure they are testable, measurable, and achievable.

2) Supports the T&E Manager and System Evaluator by providing input to EF development with a focus on the QT primary and secondary data source assignments for requirements verification.

3) Provides input as requested by the PMO or the T&E Manager for the PMO-managed IMS concerning QT test activities, timelines, and predecessors.

4) Provides QT inputs to the TEMP and EF as requested by the PM or T&E Manager.

5) For deployed systems, reviews and provides feedback to the CM Team on system change documentation as it relates to a potential Regression QT (RQT).

6) Coordinates with the System Evaluator and PMO to identify RQT test scope for change requests. Provides input as requested to the System Evaluator for the development of a DTS.
7) Develops and distributes the test plans and reports for QT and RQT results.
8) Executes all QT and RQT test activities

2.5 Designated Government Certification Agent

(1) Reviews all CERT-related operational, technical, and functional requirements to ensure they are testable, measurable, and achievable.

(2) Supports the T&E Manager and System Evaluator by providing input to EF development with a focus on the CERT primary and secondary data source assignments for requirements verification.

(3) Provides input as requested by the PMO or the T&E Manager for the PMO-managed IMS concerning CERT activities, timelines, and predecessors.

(4) Provides CERT inputs to the TEMP as requested by the T&E Manager.

(5) For deployed systems, reviews and provides feedback to the CM Team on system change documentation as it relates to CERT.

(6) Provides input as requested to the System Evaluator during the development of the DTS.

(7) Develops and distributes the CERT Test Plan, CERT QLR, CERT Emerging Results Report, and CERT Final Report.

(8) Executes all Certification activities for Readiness Assessments, Certification Readiness Tests and Certification Tests.

(9) Provides input, as requested, to the System Evaluator for the development of the CERT Letter Concurrence Memorandum.

(10) Provides input into the threat working group to define the threat/threat set required to execute CERT against applicable requirements and detection standards.

(11) Develops the CERT Management Plan in collaboration with the PMO and T&E Manager.

(12) Supports vendor TIMs upon request of the PM on areas pertinent to CERT and Certification Readiness Testing.

(13) Advises on potential detection impacts with respect to changes in the detection standard or functional requirements associated with explosive and PI detection.

2.6 T&E Stakeholder Organizations

The following are TSA organizations that provide additional input and support to T&E efforts.

2.6.1 APM/PEO

The PEO is the organization within APM in which the PMOs are functionally aligned. The PMOs are segmented within Portfolios with an identified PM to oversee each acquisition program. The PMO is responsible for the overall management of the program to include schedule, budget, and technical capability against requirements.

2.6.2 APM/Capability and Acceptance Management Branch

The Capability and Acceptance Management Branch (CAMB) within APM is responsible for overseeing the capability acceptance process, which manages all donation activities of security equipment for TSA. CAMB provides guidelines for donors, ensures the donation activity has an appropriate financial analysis and business case, determines whether the donated equipment meets TSA guidelines, and ensures donated equipment receive satisfactory third party AT prior to operational use.

2.6.3 APM/Deployment and Sustainment Division

The Deployment and Sustainment Division (DSD) provides site characteristics and relevant historical data to inform the site selection process and supports the installation and integration of systems at operational sites as needed.

2.6.4 CAE Staff

The CAE staff provides acquisition assistance to the PMO and the ITA. The CAE staff guides the PMO through the acquisition process to successfully navigate all ADEs and coordinate TSA ADMs. The CAE staff, at the time of this guidebook revision, are organizationally aligned within the APM/Acquisition Advisory Division (AAD).

2.6.5 Contracting and Procurement

Contracting and Procurement (C&P), together with the PMO, serves as the liaison between TSA and the vendor. C&P is responsible for managing the overall procurement process, coordinating industry days, issuing contract awards, and the release of qualification documentation. C&P supports the PMO in the development and execution of the program acquisition strategy.

2.6.6 IT/IAD

IT personnel provide expertise in areas associated with IT and cybersecurity. IT/IAD, or alternate entity depending on the TES, provides general cybersecurity T&E input to the System Evaluator. This includes activities such as development of threat assessments, conducting Cooperative Vulnerability and Penetration Assessments (CVPAs) and Penetration Tests, results analysis, and development of reports. The ITA is responsible for the execution of the AA.

2.6.7 IT/Governance, Risk, and Compliance

The Governance, Risk, and Compliance (GRC) Division within IT, manages the overall risk and compliance determinations of TSA systems. As it relates to T&E, GRC conducts security controls assessments in support of authority to operate or risk acceptance memorandum decisions, which must be in place prior to a test activity of a TSA-connected system. Further, the GRC concurs with plan of action and milestone vulnerability closure requests upon review of closure evidence and supporting materials.

2.6.8 Intelligence and Analysis

Intelligence and Analysis provides the PMO, requirements sponsor, and T&E organizations with intelligence-based threat information (i.e., threat actors, vulnerabilities, adversary tendencies and preferences) in support of the system threat assessment and overarching TES.

2.6.9 Occupational Safety, Health, and Environment

Occupational Safety, Health, and Environment (OSHE) provides support to the T&E organizations by performing, or supporting, safety assessments for candidate TSE. OSHE provides findings, impact assessment, and recommendations related to issues discovered.

2.6.10 Requirements and Capabilities Analysis/Analysis and Engineering

Requirements and Capabilities Analysis (RCA)/Analysis and Engineering Directorate supports T&E by providing analysis, threat and risk assessments, requirements development, and acquisition documentation development such as the Mission Needs Statement (MNS), Concept of Operations (CONOPs), and Operational Requirements Document (ORD).

This Directorate also supports RCA's mission by managing and/or coordinating demonstrations of emerging technologies and support early identification of capabilities and limitations. When requested, the T&E Division may conduct one or more early test activities (e.g., OUEs, Data Collection Activities) in support of these initiatives.

2.6.11 RCA/Capabilities Management and Innovation

RCA/Capabilities Management and Innovation Directorate personnel serve as the capability managers (User Representatives) for acquisition programs. The User organization is responsible for approving and or concurring with acquisition documentation such as the MNS, CONOPs, ORD, and TEMP. The User organization provides the operator’s perspective throughout the T&E process, to include providing input to any observed T&E deficiencies, approves test articles used during testing, and provides critical inputs to the OT site selection process. The ITF leads technology exploration and R&D initiatives. When requested, the T&E Division may conduct one or more early test activities (e.g., OUEs, Data Collection Activities at the TSIF) in support of these initiatives.

2.6.12 Training and Development

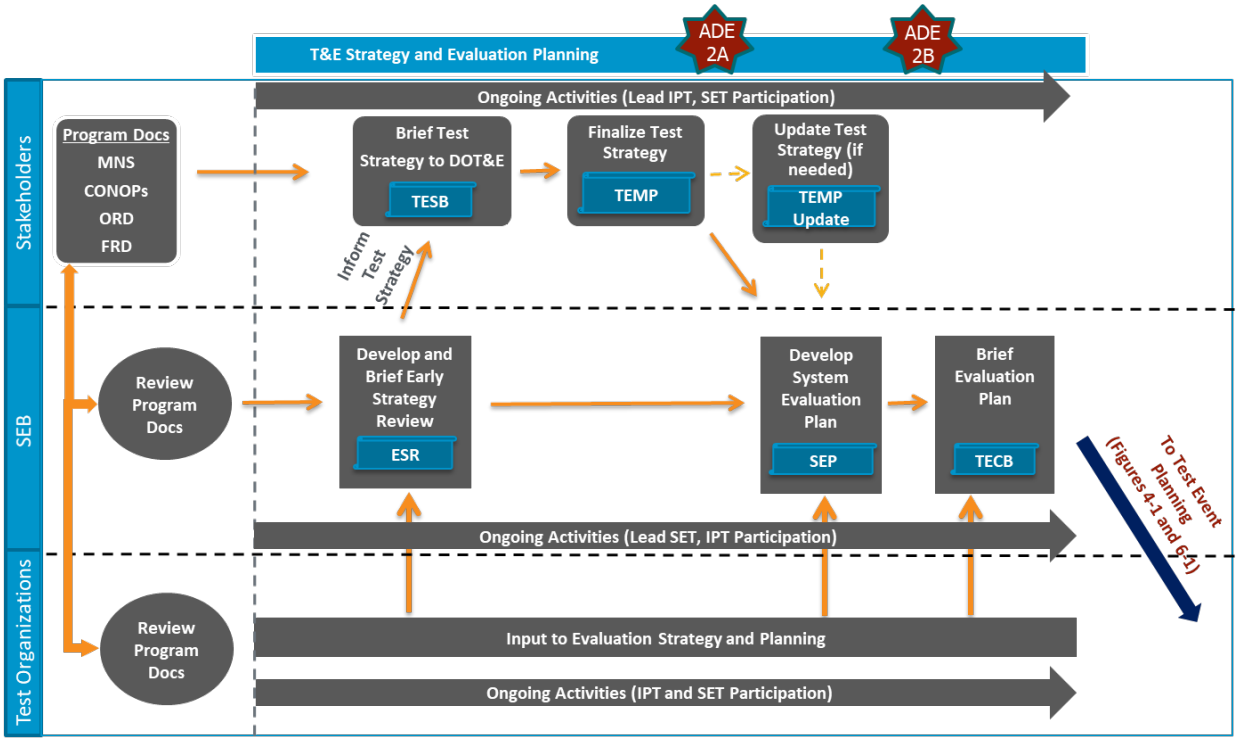
Training and Development is responsible for coordinating with the vendor, airport TSA personnel, and the T&E IPT to prepare training curriculum and job aides prior to test execution. Training and Development personnel review vendor documentation and TSA Standard Operating Procedures (SOPs), develop the curriculum, coordinate with the user organization and each test site to determine training needs, and administer the training.

3.0 T&E STRATEGY AND PLANNING

The following sections describe the procedures for the development of the TES and evaluation planning in support of Acquisition Program T&E. Efforts in support of non-acquisition activities (e.g., R&D initiatives) typically do not include the development of a TES and proceed directly to test event planning. These efforts include RCA/ITF demonstration projects. Additional information concerning these activities can be found in the TSAAM.

The PMO leads the development of the TES early in the acquisition process in parallel to requirement development and prior to ADE-2A. The TEMP describes the TES and is a key reference point for the System Evaluator in their development of the SEP. **Figure 3-1** illustrates TSA TES and evaluation planning activities.

Figure 3-1: TES and Evaluation Planning Process Flow



3.1 T&E IPT

To ensure coordination of the acquisition program and T&E activities, the PMO forms a T&E IPT that includes representation from the user community, the ITA, and other acquisition stakeholders. The PM charters the T&E IPT and has the overall responsibility for coordination of T&E activities. The Program T&E Manager leads the T&E IPT upon delegation by the PM and is responsible for soliciting T&E IPT input to develop the TES and TEMP.

3.2 System Evaluation Team

The primary objective of the SET is to provide the coordination necessary on behalf of the ITA to execute T&E activities per the TEMP. The System Evaluator is the SET Chair and forms the SET as the TEMP nears completion or in parallel to acquisition documentation (e.g., requirements) development in cases where there is no established T&E IPT. The SET's individual members should:

- Be empowered by their parent organizations to make decisions, and keep their organization informed of issues discussed by the SET.
- Plan, execute, and report test activity results, progress, and risks to the SET chair.
- Communicate and maintain awareness of the T&E schedule and milestones to ensure timely completion of T&E activities.
- Provide input, feedback, and concurrence/non-concurrence as required for all T&E documentation requiring SET approval.
- Provide input in support of site selection.
- Provide input and complete tasks as listed in the Qualification Test Readiness Review (QTRR) and OTRR.

SET participating organizations will typically consist of the PMO, SEB, OTB, DGCA, TTB, Cybersecurity Test Teams, DOT&E, and the User Representative. The System Evaluator will expand SET membership as needed to ensure engagement of all necessary parties.

3.3 Reviewing and Assessing Requirements

Working within the T&E IPT, the ITA provides early and continuous feedback to RCA and the User Representative on the testability and measurability of operational requirements, to include the Key Performance Parameters (KPPs) as documented in the ORD. Similarly, the T&E Manager works with the ITA to solicit FRD feedback prior to signature. The test organizations also comment on other requirements documents when appropriate such as detection standards and interface control documents, which specify functionality for system interoperability.

When reviewing operational and functional requirements, T&E Teams consider the following:

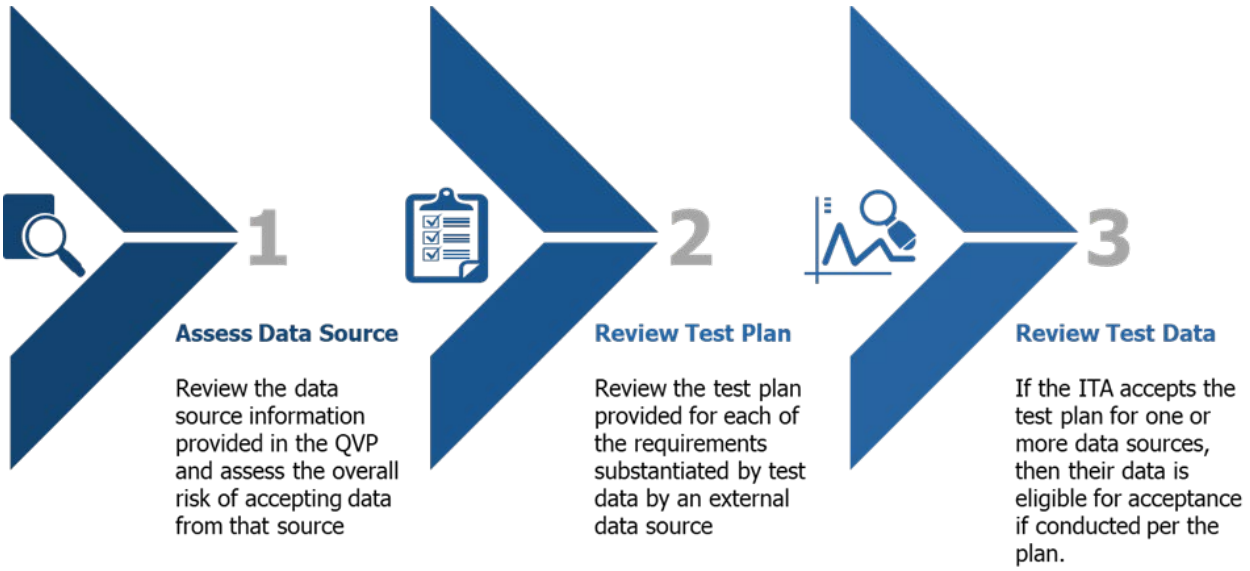
- Whether requirements are clearly defined, achievable, testable, and measurable.
- Available test capabilities and limitations as it relates to the evaluation of requirements.
- Major operational risks, changes, or impacts.
- Safety and security risks.

3.4 Use of Third Party Testing in a System Evaluation

The System Evaluator may consider external data sources (e.g., third party test data) in a system evaluation to reduce the testing performed by the ITA and/or add additional confidence to test results. The ITA's decision to accept an external data source in its evaluation is separate from the

PMO's decision on whether to accept a vendor as part of TSA's qualification process. Generally, the ITA first reviews vendor-provided data source information and test plans in the Qualification Verification Package (QVP) and then reviews test data from these data sources in the Qualification Data Package (QDP) as illustrated in **Figure 3-2**. The TSA Third Party Testing Framework defines this process in detail.

Figure 3-2: ITA Review of External Data



3.5 Developing Evaluation Criteria

The evaluation of Operational Effectiveness, Suitability, and Resilience is dependent on the resolution of User Representative-identified Critical Operational Issues (COIs). COIs are introduced in the ORD and represent key operational concerns, with standards of performance that if met, signify that the system is operationally ready to be fielded.

Upon review of the ORD, the System Evaluator may identify one or more Additional Issues (AIs). AIs are key operational concerns that have not been explicitly designated by the User Representative as a COI, however, are necessary for assessment per the judgement of the System Evaluator. Each COI/AI is associated with one or more Critical Operational Issue and Criteria (COICs) and/or AI criteria. COICs are the standards of performance (criteria) for each COI, developed by the System Evaluator, that must be answered to determine if the system is ready to enter full-rate production.

For each criterion, the System Evaluator derives supporting measures used to assess the system's ability to satisfy the criterion and in turn, the COI/AI. The System Evaluator uses KPPs, when possible, as criteria that directly support the evaluation of a COI. Characteristics of good COICs/AI criteria are:

- Measurable and can be evaluated as met or not met.

- Avoid terms that could be misinterpreted during the analysis and/or evaluation.
- Associated with one or more measures that reflect the minimal system acceptable performance for entry into procurement (i.e., threshold values).

Figure 3-3 depicts examples of COICs (phrased as questions) and derived measures.

Figure 3-3: Example Criteria and Derived Measures

<table>
<tr><th colspan="4">Operational Effectiveness</th></tr>
<tr><td colspan="2">Does the system perform effectively in the target environment?</td><td colspan="2">• Probability of detection
• False alarm rate</td></tr>
<tr><th colspan="4">Operational Suitability</th></tr>
<tr><td>Is the system interoperable with other systems and protocols?</td><td>• System interface and data requirements
• Installation and integration ease</td><td rowspan="2">Will the system be reliable, maintainable and available in the target environment?</td><td rowspan="2">• Operational Availability
• Mean time between failures
• Mean time between critical failures
• Mean time to repair
• Mean down time
• Mean time between maintenance actions</td></tr>
<tr><td>Are Human Systems Integration attributes appropriate for the target environment?</td><td>• Usability
• Training
• Staffing/Manpower
• Safety</td></tr>
<tr><th colspan="4">Operational Resilience</th></tr>
<tr><td colspan="2">Does the system provide sufficient resilience to maintain operations in the checkpoint or checked baggage screening environment?</td><td colspan="2">• System Design (Resilience)
• Survivability</td></tr>
<tr><td colspan="2">Does the system satisfy the mission while under duress from offensive cyber-attacks?</td><td colspan="2">• Accounts and access
• Assessment of System Hardening
• Assessment of Data Integrity
• Assessment of Data Exfiltration</td></tr>
</table>

3.6 TES Development

For major programs (non-delegated systems), the PM, T&E Manager, and ITA jointly prepare a TES briefing in alignment with the program's acquisition strategy. The System Evaluator is responsible for providing an ESR briefing to the Executive Director, ITA and Executive Director, PEO a minimum of 21 calendar days prior to the TES briefing to DOT&E. An ESR is not required for non-major, major program (post-FOC delivery), and major programs (delegated systems).

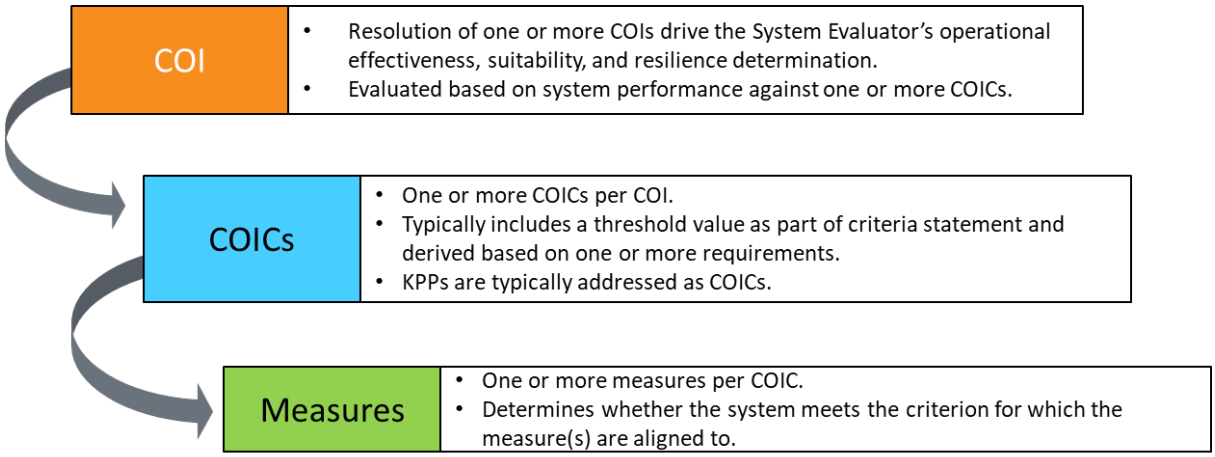
The ESR is a concise briefing summarizing the TES and emphasizing best practice T&E principles that enable speed to field and increased performance by discovering problems early.

Upon completion of the ESR and 60 days prior to submission of the TEMP, the PM and T&E Manager brief the TES to DOT&E for major programs (non-delegated systems) or to the CAE for non-major programs, if desired by the CAE. Upon request by the PM and/or T&E Manager, the System Evaluator and/or Test Directors will brief the details of the test events required to support the TES. It is critical for all relevant stakeholder groups (e.g., User Representative, T&E

organizations) be present for the TES briefing to answer any questions. The TES briefing provides the PMO and T&E stakeholders with input for incorporation during TEMP development. Within 10 calendar days of the TES briefing, the DOT&E will provide a TES Brief Memorandum to document recommendations and guidance for inclusion within the program's TEMP.

Figure 3-4 shows the hierarchical relationship between COIs, COICs, and measures.

Figure 3-4: Relationship of COIs, Criteria, and Measures

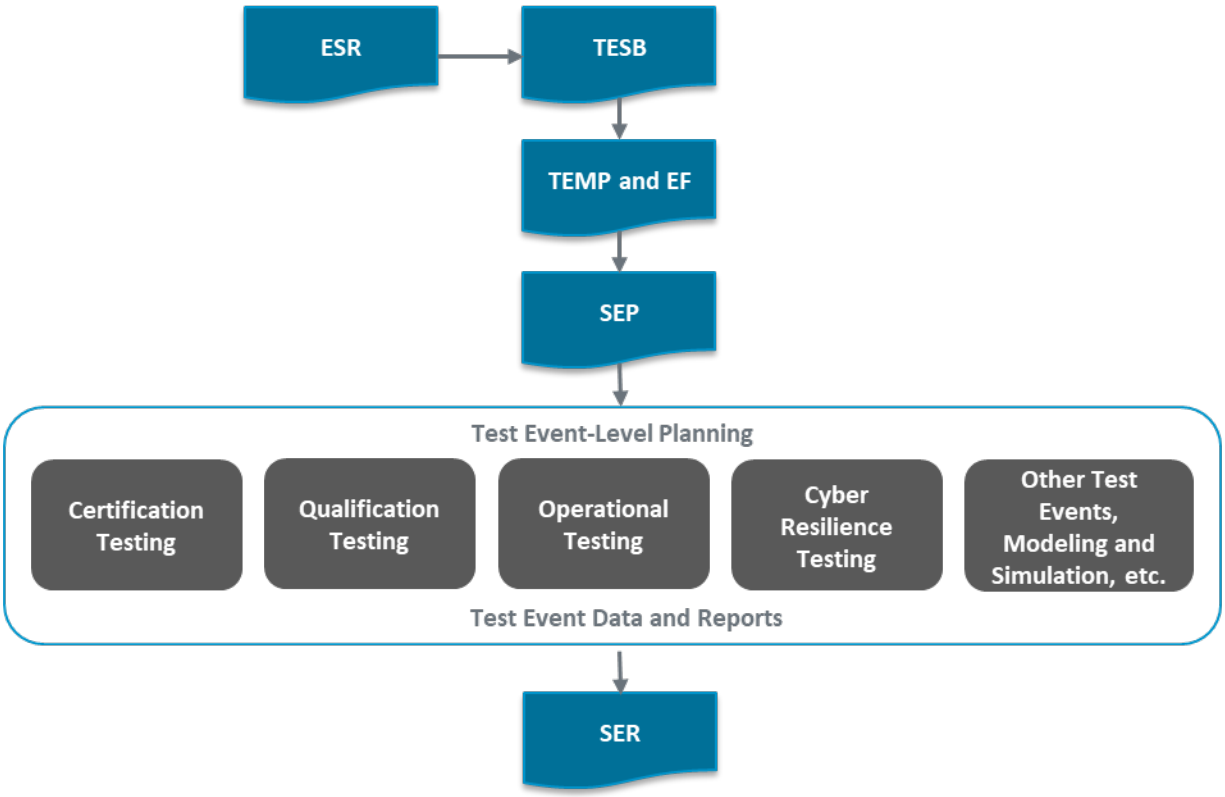


3.7 TEMP Development

The T&E Manager, in support of the PM and in coordination with the T&E IPT, develops a draft TEMP in parallel to the development of requirements, and obtains final approval from DOT&E 30 days prior to ADE-2A. The T&E Manager follows the guidance in *DHS Instruction Guide 026-06-001-01, Test and Evaluation Master Plan (TEMP),* dated October 03, 2018, when developing the TEMP. The CAE concurs with the TEMP for major programs (non-delegated systems) prior to routing to DOT&E for final approval. The CAE approves the TEMP for non-major programs.

The TEMP describes the test strategy as summarized in the TES briefing, includes an EF that identifies the data sources to be used to evaluate the operational and functional requirements, and the sequence of test activities necessary to complete the evaluation. The ITA provides inputs to the TEMP with a specific focus on the EF, Failure Definition and Scoring Criteria, and Integrated Test and Evaluation Activities. **Figure 3-5** illustrates the general process and documentation hierarchy for a system, beginning with the ESR and culminating in the development of the SER.

Figure 3-5: TEMP to Reporting Hierarchy



The T&E Manager may update the TEMP, as needed, prior to ADE-2B and anytime changes to the program (e.g., Acquisition Strategy, program mission, key operational requirements) necessitate a change in the overarching TES. The TEMP revisions should receive the same endorsements and approvals as the initial version. If only the EF changes, the T&E Manager should communicate these changes to DOT&E and transmit the EF revision to all parties who previously received the approved TEMP. Under these circumstances, a TEMP re-approval is not necessary unless requested by DOT&E. The PM submits the initial TEMP to DOT&E for approval a minimum of 30 calendar days prior to ADE-2A.

3.7.1 Evaluation Framework

To ensure that the requirements decomposition is complete, the PMO develops a Requirements Traceability Matrix (RTM), which provides a method for tracking that all requirements in the ORD have been decomposed within the FRD. The RTM includes the assignment of a suggested verification method (inspection, demonstration, test, or analysis).

The System Evaluator uses the ORD, FRD, and RTM (if available) to develop a Requirements Crosswalk Matrix (RCM) and provides the RCM to the Program T&E Manager as an input to the formation of an EF. The development of the RCM portion of the EF begins with the System Evaluator correlating FRD requirements to ORD requirements (or confirming the PMO's correlation of requirements if provided through the RTM), to measures, to COICs, and to COI.

This traceability exercise enables the System Evaluator to produce a consistent, fully-justified set of operational measures, in alignment with the COIs, as the foundation for the evaluation.

The System Evaluator, with input from the various test organizations, then identifies the primary (P) and secondary (S) data sources for verifying each requirement. The System Evaluator considers all data sources when making the primary or secondary assignment to include, but not limited to, CERT, QT, OT, Integrated Test Event, Safety Assessments, and Cybersecurity Assessments (e.g., CVPA, AA).

The System Evaluator also considers whether they can use data from previous test events and/or external sources to demonstrate requirements compliance. The System Evaluator should consider all potential sources of data in this regard, to include data collected in support of RCA technology demonstrations and OAs. In these cases, the System Evaluator ensures test conditions and system configurations are representative and clearly documents the existing data source (e.g., Year, Report/Event Name). Primary data are generally the source for determining whether a requirement is satisfied. Secondary data provide additional information that can influence the System Evaluator's judgment on whether a system has satisfied a requirement.

After the System Evaluator finalizes and provides the RCM to the Program T&E Manager, the T&E Manager then adds components to the RCM such as test conditions and decision support questions to form the EF. The T&E Manager incorporates the EF into the TEMP.

The RTM and EF may require an update if the PMO initiates or updates an acquisition strategy in order to provide new or enhanced capability. If the PMO issues additional technical and functional requirements to define the new of enhanced capability, the T&E Manager updates the RTM and EF. The T&E Manager distributes the revised EF to the TEMP stakeholders. The System Evaluator updates the SEP with the revised EF and alerts the Test Branches so they can revise appropriate test plans.

3.7.2 Modeling and Simulation

Modeling and Simulation (M&S) planning typically begins during TEMP development to ensure the T&E strategy includes M&S if required. M&S is the use of a physical or logical representation of a system to generate data to support the test and analysis process. As an example, an emulator is used to reduce the time and effort required for fielding new detection algorithms. The primary function of the emulator is to imitate the explosive detection capability of the scanner by processing previously scanned image files.

System Evaluators can use M&S as an additional data source to supplement test data but generally not used to replace QT or OT in the TES. During the planning process, the System Evaluators may use M&S for:

- Prediction of system performance.
- Stressing the System Under Test (SUT) to simulate high-load environments.
- Assessment of system capabilities in situations where testing in the operational environment is not feasible.

Prior to use, the System Evaluator should ensure the model is accredited per the guidance in the *TSA Verification, Validation, and Accreditation (VV&A) Policy,* dated March 27, 2014.

3.8 System Evaluation Plan

The System Evaluator begins development of the SEP in parallel to the TEMP review process. While the TEMP provides the overall scope and strategy for T&E, the SEP dictates how the evaluation will be accomplished. Alignment is critical to ensure evaluation planning supports the TES. The SEP details the measures and analysis methodologies the System Evaluator will use to evaluate the system's Operational Effectiveness, Suitability, and Resilience. Additionally, the SEP:

- Describes how the planned test events support the evaluation of COICs and measures.
- Contains the RCM portion of the EF.
- Includes T&E limitations. These limitations must not rationalize why the T&E Team will not assess requirements, but rather, must present a suitable alternative test methodology.

The System Evaluator typically updates the SEP whenever the PM or T&E Manager updates the TEMP and may initiate an update independent of the TEMP if significant program changes occur for new or enhanced capability which may include additional requirements added to the FRD. The SET provides feedback prior to final SEP approval. The System Evaluator gains concurrence on the SEP from the SEB, OTB, and TTB Managers, and final approval from the Executive Director, ITA.

3.9 Test and Evaluation Concept Briefing

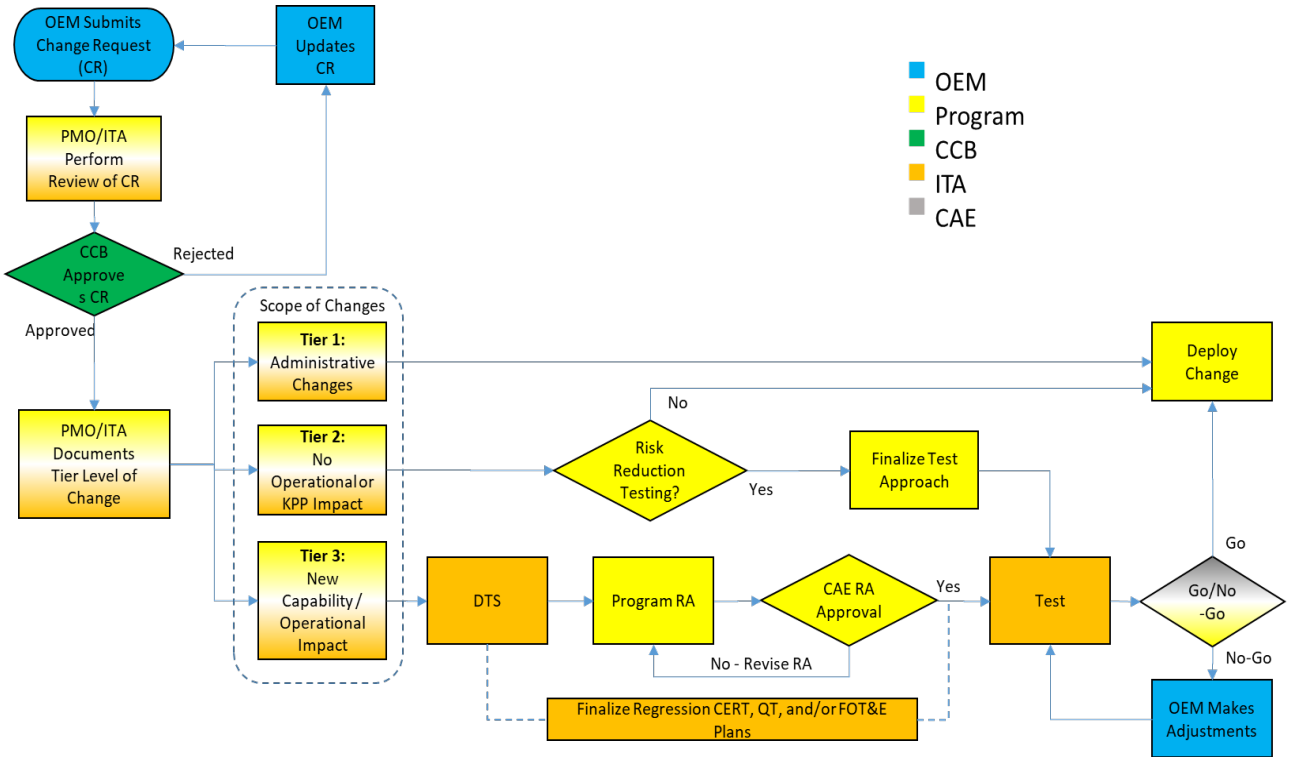
Once the TEMP is approved by DOT&E (or the CAE for non-major programs), and the SEP has been drafted, the System Evaluator presents the evaluation plan to DOT&E in the form of a TECB. The briefing describes the system, the COICs, measures, test objectives, overall test methodology, test event entrance and exit criteria, test durations and sites, and other details that support the various test events. While the TECB provides additional detail on the test events introduced in the TEMP, its focus should be the OT event. The content presented in the TECB should be consistent with the SEP and guide the development of the OTP. For major programs (non-delegated systems), the System Evaluator presents the TECB to the DOT&E 120 calendar days prior to the start of OT and 60 calendar days prior to OTP submission. For non-major programs, the System Evaluator presents the TECB to the Executive Director, ITA. Major programs (delegated systems) and major programs (post-FOC delivery) typically do not require a TECB.

3.10 Determining the Scope of Testing After a System Change

Changes to deployed, previously evaluated systems may occur due to several reasons such as deficiency correction, operating system upgrades, updates for an end-of-life hardware or software component, and/or upgrade the system's detection algorithm. In addition, the acquisition of new or enhanced capabilities may result in system changes requiring re-evaluation. When these changes occur, it is critical for the ITA to assess the change package and determine

the level of regression testing necessary to ensure expected performance is maintained. **Figure 3-6** illustrates the changes to deployed systems process below. The *Managing Changes to Deployed TSA Systems* ADM, dated February 12, 2019, originally documented this process, updated in Figure 3-6 to reflect the scoping of changes and the various actions that result based on the scope/tier designation.

Figure 3-6: Changes to Deployed Systems Process



The System Evaluator and Test Directors (e.g., QTD, OTD) review change packages upon initial distribution by the Configuration Control Board (CCB). The purpose of this review is twofold. First, the T&E Team provides information that may be used by the CCB to inform its decision whether to approve the change package. Second, the T&E Team reviews to better understand the scope of the changes and to determine the tier value corresponding to the change(s). During this review the System Evaluator and Test Directors should request any additional clarifying information from the vendor through the CCB Point of Contact (POC). They should also ensure all changes listed in the Request for Deviation (RFD) have been considered.

As part of the ITA's review and analysis of the change package, the System Evaluator should consult the various Test Directors (e.g., QTD) to ensure the ITA has a common understanding of the change and to discuss any potential required regression testing. Change packages may have a single functional purpose; however, a number of underlying changes may have been necessary to achieve that purpose, or the vendor may have made unrelated system changes that they are submitting as part of the change package. The System Evaluator may also perform an initial assessment of the proposed changes against the measures listed in the system's EF to understand the impact of the change against the previously evaluated system.

Once the review and analysis are complete, the ITA and PMO assign a tier designation for the change package no later than 7 calendar days after Change Request (CR) approval. The tier is a designation of the magnitude of the change as described in **Table 3-1**. This tier designation is solely to assist in test scope determination. It should not be confused with the formal CM CR classification types of critical, major, and minor.

If the PMO and ITA do not agree on a common tier designation, and a Tier 3 change is recommended by either party, the change package will receive a Tier 3 designation as a DTS and PMO Risk Assessment will be needed to determine the path forward. The following table lists the three tiers and ITA actions for each.

Table 3-1: Change Package Tier Designations

Tier #	Description	ITA/T&E Role
1	Administrative changes that do not impact operations such as changing/applying labels and effectivity changes for the systems receiving the change.	None. The PMO proceeds to deploy the change.
2	Minor changes that do not have the potential to impact a system's operational capability. Changes in this tier include end-of-life replacement components that are supposed to behave in the same manner as already deployed components.	The ITA does not formally evaluate Tier 2 changes and does not produce a SER. The PMO however may request assistance from the QT Branch to conduct testing for risk reduction purposes.
3	New or updated capabilities that may have an operational impact on system performance. Common operational areas potentially impacted include, but are not limited to, detection, false alarm rate, throughput, RMA, core system-specific functions (e.g., identification document authentication), safety, human-systems integration, and/or cyber resilience.	The System Evaluator develops a DTS. The System Evaluator uses the DTS to determine whether the change impacts the results of a previous T&E. In the DTS, the System Evaluator examines the change against the EF to determine impact and any required regression testing. The Test Branches must ensure alignment of any test plans (e.g., Regression Qualification Test Plan [QTP], Follow-on Operational Test Plan [FOTP], CERT Plan) with the DTS. This alignment between the System Evaluator and Test Branches ensures the SER is robust and complete.

For Tier 3 changes, the System Evaluator distributes the DTS to the SET for review and feedback. The System Evaluator then sends the DTS to the SEB Manager for review and then to the Executive Director, ITA for approval no later than 21 calendar days after the Tier 3 designation (28 calendar days after RFD approval). Upon approval, the System Evaluator then provides the DTS to the PMO to inform a program-level risk assessment. The PMO submits the risk assessment to the CAE for approval.

4.0 DEVELOPMENTAL, CERTIFICATION, AND QUALIFICATION TESTING

TSA performs Developmental Testing (DT) and Data Collection Activities of prototype systems in support of R&D, CERT of detection-representative systems to verify system detection performance, and QTs of production-representative systems to support qualification as described in the TEMP. These events provide a verification of system conformance to functional specifications, in a laboratory environment. The following paragraphs further describe these events:

- TSA performs DT and Data Collection Activities collaboratively with TSA stakeholders and vendors to help identify system performance and deficiencies early to assist in system maturation, ensure vendor products meet TSA expectations, assist in requirements development, and determine system capabilities and limitations before conducting OUEs in the field. These events are flexible in test scope and typically performed in support of sponsoring organizations (e.g., RCA) or to assess a vendor's technical maturity through witness testing at the vendor factory prior to the PMO accepting the vendor for further testing by TSA. TSA typically conducts DT and Data Collection Activities at the TSL or the TSIF. TSL DT activities primarily consist of readiness testing to assist in the maturation of explosives-based detection algorithms. TSIF-based DT and Data Collection Activities may include readiness testing for detection algorithms against PI threats in addition to non-detection requirements.
- CERT verifies threat detection performance, typically probability of detection and false alarm rate metrics. TSA systems designed to detect explosive materials typically undergo CERT at the DGCA facilities (e.g., TSL), whereas CERT for non-explosive detection is also conducted at the TSIF for some technologies. Once successful, TSA certifies detection standard compliance by issuing a certification letter to the vendor for the system configuration tested. In these instances, the ITA provides the Executive Director, PEO with a CERT letter concurrence memorandum supporting the issuance of the letter. Additional information concerning CERT can be found in the TSA Transportation Security Equipment Certification Policy.
- QTs provide an analysis of whether the system complies with the technical requirements defined in program requirements documents (e.g., FRD), in a laboratory environment. QTs typically assess the requirements not related to detection of explosive materials. QT reports align with the TEMP and SEP and serve as an input to the SER. As a result, the QT may include studies and excursions (e.g., PI detection study) as documented in the SEP. TSA typically performs a QT at the TSIF. A well-planned and executed CERT and QT program supports the determination of whether a system meets user needs and can proceed to operational use.

Additional objectives of the DGCA and/or TTB include:

- Review and analyze vendor-submitted data packages (e.g., QDPs, PI certification data packages). Provide comments and disposition to the PMO.
- Perform regression CERT and/or a QT, in response to approved vendor change packages.
- Perform engineering analysis on vendor-submitted CRs for requirements and CM compliance, and to ensure the change package contains sufficient information to determine the effect of the change on system functionality and operation. The DGCA and TTB use this information to establish the as-tested baseline configuration.
- Identify and describe system design, usability, and other related risks.
- Working with OSHE, assess the safety of the system to ensure its safe operational use. The intent is to ensure that systems are sufficiently free of hazards to prevent harm or injury to test personnel, typical users, and the public in operational environments.
- Support assessments to verify system-of-systems interoperability. This includes coordinating with other organizations to facilitate assessments. For example, the TTB would coordinate with IT/IAD to perform a CVPA.

4.1 Test Event Overview

QT events support the system evaluation as described in the TEMP. Data Collection Activities support all other requests for test data and results. Policy guidance for these events can be found in *TSIF Events Management, TSA MD 2600.3,* dated April 27, 2022. **Table 4-1** provides additional information for these events.

Table 4-1: Developmental / QT Events

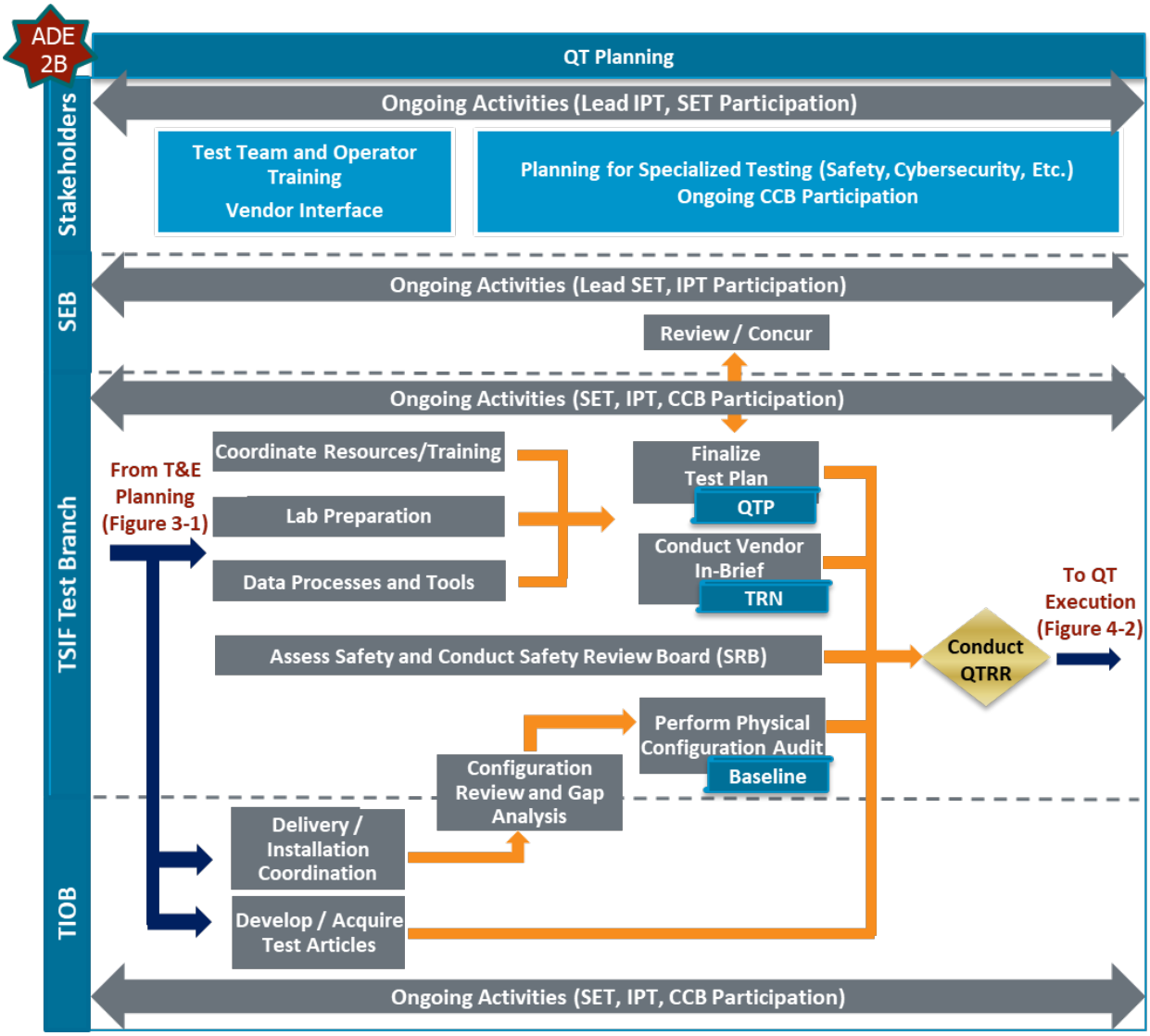
Test Type/Purpose	Additional Detail	Plan	Report
QT The formal verification of system design against the system requirements contained in the FRD, which provides confidence that the system will deliver the desired capabilities in an operational environment.	• May include verification of non-FRD requirements as documented in the EF. • Includes verification of critical technical parameters. • Provides performance metrics to advise on system readiness to enter OT. • Includes excursions and studies (e.g., PI detection study).	QTP	QLR, Final Results Summary (FRS), or Qualification Test Report (QTR)
RQT RQTs verify vendor implementation of system updates to characterize the change's impact on system performance and compliance with requirements.	• Testing resulting from vendor changes in approved CRs. • Determine adequacy for fielding the system configuration or to enter Follow-on Test and Evaluation (FOT&E).	Regression QTP*	QLR, FRS, or Regression QTR
Data Collection Activity Test activities that support any requests for data collection outside of a formal QT. These can include ITF initiatives, integration tests, data collection to support OT and CERT, and any other ad-hoc requests to determine capabilities and limitations.	• Assess/validate CONOPs. • Intelligence-based threat mitigation assessments. • Provide insight into the human factors, usability, safety, and design characteristics of a system. • Provide input into SOP and training development.	Data Collection Activity Plan	FRS or Data Collection Activity Report (DCAR)
CVPA The CVPA assesses the overall hardening of the system in an attempt to identify and reduce vulnerable elements of the attack surface. The CVPA typically consists of automated and manual hardware and software assessments.	• Performed by TTB in either a lead or supporting role to IT/IAD. In either role, close coordination between the two groups is paramount. • Vulnerability scanning of system software, operating system, network interfaces, etc. • Light manual penetration assessment.	CVPA Plan	CVPA Findings CVPA Report

*QT efforts may include alternate, expedited methods for regression test planning if no (or minor) changes would be needed to existing test methods published in the QTP, to include email concurrence of approach and agreement on the reuse of test methods.

4.2 QT Planning

The TTB performs several planning activities to prepare for a QT event. Central to these planning activities is the review of vendor-submitted QVPs and QDPs and the development of the QTP. QDP acceptance is typically a pre-requisite to the commencement of QT at the TSIF. In depth processes for these activities are controlled by the TSIF Quality Management System, which is ISO 9001:2015 certified, and contained within the *TTB and Test Infrastructure and Operations (TI&O) Integrated Process Manual (IPM)*. **Figure 4-1** illustrates the various activities taking place during QT planning by various stakeholders.

Figure 4-1: Qualification Test Planning Process Flow



4.2.1 Planning Documentation

The QTD creates a QTP based on the TEMP, SEP, and requirements allocated to QT in the EF. The System Evaluator primarily allocates FRD requirements to the TTB; however, ORD requirements may be assigned for verification during QT when operational conditions limit the ability to collect the necessary data. The QTP describes the details of the test to include a schedule of events, safety considerations, training required, test article details, required personnel, test scenarios, data collection tools, and test methodology. The QTP also lists the expected reporting artifacts (e.g., QLR, Final Results Summary [FRS]) and delivery dates for each upon completion of testing.

As detailed in the *TSA APM T&E TSIF TEST and TI&O Quality Manual, Section 7.5.2-1 –TSIF Document Review Process,* the QTD gains initial concurrence from the System Evaluator, affirming the QTP will adequately support the evaluation prior to concurrence by the TTB Manager and approval by the Executive Director, ITA.

For regression testing or other data collection events outside the scope of the QTP, unless otherwise directed by T&E Division leadership due to the significance of the test event, the TTB Manager approves any data collection activity plan required. The System Evaluator may also allocate FRD requirements to specialized test entities (e.g., IT/IAD, OSHE). The planning documentation for the activities performed by these entities is typically outside the scope of the QTP, and developed under separate cover by those groups.

4.2.2 Coordination of System Delivery and Installation

The PMO works with the T&E Division TI&O Branch to coordinate any equipment required to be delivered to the TSIF for testing purposes. The PMO is required to work with the TI&O Test Area Manager and TSA Property Manager to complete the appropriate paperwork and coordinate the install schedule with TI&O to ensure appropriate awareness and support is in place for the delivery and installation.

4.2.3 Establishing the Configuration Baseline Prior to Qualification Testing

In order to effectively establish and manage the configuration of TSE at the TSIF, TSIF Test CM Leads must accurately understand the product structure of a system, identify critical Configuration Items (CIs), and develop an appropriate set of working documents. These high-level activities generally precede the TSIF CM audit, which must occur prior to the onset of a QT at the TSIF.

The following steps apply to all TSIF TSE with system technical and/or CM requirements, where a set of equipment vendor CM documentation is needed to establish the TSIF TSE configuration baseline prior to QT testing:

1. Obtain Vendor CM Documentation – TSIF Test CM Leads collaborate with TIOB CM, the QTD, and the PMO to obtain applicable equipment vendor CM documentation.

2. Identify and Analyze Technical Requirements and Critical Functions – Includes requirements and functional analysis and identifying top-level system functions that correlate with individual requirements.
3. Develop Draft Working Documents – Develop draft list of Test CIs, derived from the functional analysis and vendor CM documentation. The draft Test CI list forms the basis for developing, and later managing, the "As-Tested Configuration Baseline" (ATCB) of the applicable TSIF TSE system.

The ATCB CM Audit applies to mature systems that must conform to performance, contractual, and otherwise documented, technical TSA requirements. The following key activities apply to TSIF TSE that require TSIF Test CM Leads to characterize and document the physical and functional characteristics of "ATCB" TSIF TSE systems prior to a QT:

1. Pre-audit activities – May include technical review of CM documentation with equipment vendors. This activity serves to confirm and enhance TSIF Test/CM understanding of critical CI functions, system hierarchy and interfaces, software modules, etc.
2. Conduct TSIF CM Audit – Inspection of all hardware and software Test CIs to verify correct nomenclature, part number/revision, correlation to specification sheets/design drawings, software version/build number, detection characteristics, program logic controller/firmware version (as applicable), file directory location of all individual SW items, correlation to release notes.
3. Post-audit activities – The initial output after completion of the CM audit is a high-level summary of initial audit findings. Major discrepancies are noted, as well as negative impacts/risks that may occur if the discrepancies are not resolved (negotiated between TIOB CM, PMO, and equipment vendor). The final output that results from the ATCB CM Audit is the compilation and delivery of the in-depth ATCB CM audit report for inclusion in test report documents.

The ATCB CM Audit report is used as the basis for defining the APM CCB production Master Configuration Items List (MCIL) (or APM production MCIL) for systems awarded a purchase/deployment contract post-ADE-3 decision making.

If the DGCA certified the TSE prior to the QT, an electronic copy of the DGCA's approved Developmental Baseline CM audit results may be provided for inclusion with the TED/TSIF ATCB CM audit report. The TIOB CM Manager is the final approval authority for the ATCB. The TIOB CM Manager maintains this baseline throughout the developmental process.

The *TSIF Test Branch TSE Configuration Management Plan,* dated June 27, 2022, contains specific information that defines how T&E Division/TTB establishes the ATCB. The *Configuration Management Plan for OAPM,* dated August 31, 2018, contains additional information on the establishment of the CM product baseline – termed the 'PBL,' established after contract award.

4.2.4 Test Readiness Notification

The QT Test Readiness Notification (TRN) serves as a notice from the vendor that the system has been installed in the approved configuration, fully functions as intended, and is ready for QT.

Additionally, the QT TRN includes the rules of engagement for a vendor, with respect to system access during QT and maintenance, to ensure test integrity. Typically, the vendor signs the QT TRN immediately following system installation once the system is operating as intended by the vendor.

TSA requires a vendor agent to formally sign the QT TRN. This agent must have the authority and knowledge to verify whether the system has been installed in the approved configuration, fully functions as intended, and is ready for QT. The TTB submits the QT TRN to the PMO and vendor for record keeping.

4.2.5 Threat Items for CERT

In accordance with the TSA TSE Certification Policy, the PMO and ITA endorse the threat set (explosive or PI) used for CERT prior to final selection by the User Representative (Capability Manager). If there is an update to the detection standard, or if the T&E IPT determines a change in the threat set is required due to the threat environment, the T&E IPT should reaffirm the threat set and receive endorsements from the PMO and ITA with the User Representative making the final selection. The T&E IPT should monitor the threat set to ensure it remains valid over time. Any threat set update receives the same endorsements and approval as previously listed.

4.2.6 Test Article Selection and Development

Test articles used during QT vary by technology, from baggage articles with explosive simulant threats to fraudulent and authentic identification documents. The TIOB and/or TTB (test-dependent) develops Stream-of-Commerce (SOC) representative test articles in order to simulate operational conditions for scenarios that assess areas such as system false alarm rate and processing time.

The TTB and TIOB meet with appropriate organizations to assist in the selection of threat articles. These organizations can include the SEB, User Representative, intelligence agencies, other DHS agencies, and expert groups within and external to TSA that can provide an expert opinion on whether the articles are representative of the threat posed by the adversary.

When high fidelity test articles are required in support of a QT, the TIOB Team develops the test articles in accordance with the TSA VV&A Policy and the IPM, Section 9 (Test Articles) to ensure that the test articles are developed and configured to meet requirements (verification) and are an accurate representation of the operational environment (validation). TIOB builds the test articles per the design specs outlined in the Test Article Request Form, submitted by the initiator. The developing agency, typically the TIOB and/or TTB, performs verification and validation. Once verification and validation are complete, the System Evaluator determines whether the articles are acceptable for their intended use (accreditation decision) in the form of an accreditation memorandum.

4.2.7 Test Tool Development and VV&A

Early in QT planning, and through continuous improvement projects, the TTB determines the test tools and instrumentation needed to support T&E. These test tools can range from automated

data collection and analysis software to robotics used to perform constant tasks to stress system use. The initiator first creates a "Test Tool Scope Summary" to initiate a test tool development project. This defines the background, user needs, the proposed solution, deliverables, and timetable. Once the Scope Summary is approved, the TTB assigns a developer. Then the initiator develops the requirements document used for "verification" (as part of the V&V process). The TTB creates a validation plan to ensure the test tools will meet the criteria listed in the test tool document. The validation plan includes the number of samples needed and the type of data required to be collected. Based on these attributes, the TTB develops the product, or acquires the necessary materials, and runs the tool through a sample of data to determine results consistency and compliance with pre-approved criteria (validation). At the System Evaluator's discretion, SEB accredits the test tools via an accreditation memorandum if the test tools will produce data in support of a requirement in the SER.

Additional information can be found in the IPM, Process PM10-P01-v3.2, TSA TSIF Test and TI&O Test Tool Lifecycle Process.

4.2.8 Coordination with Supporting Organizations

Some QT scenarios in the QTP may require a Transportation Security Officer (TSO) to operate the TSE to best represent the TSE's performance when used in its intended environment (e.g., PI detection study). It is the responsibility of the QTD to begin coordination with organizations that will be providing operators for testing early in the development of the QTP. The initial coordination informs the organization of the need and lowers the risk that operators will not be available when the test dates are finalized. The QTD informs the System Evaluator during the SET meeting of any issues in obtaining TSOs along with a mitigation plan.

The System Evaluator, working with the test organizations, may determine the need for other organizations to support the QT event. These organizations may include IT/IAD for cybersecurity requirements and OSHE for safety requirements. These assessments generally occur at the TSIF once the TSE is installed, however, may occur remotely dependent on the nature of the requirements. It is the responsibility of the PMO to schedule with the necessary organizations, and the QTD to coordinate with PMO and the organization to ensure access is given to conduct their assessment.

The QTD, through coordination with the PMO, may require the vendor to support one, or all, of the following activities:

- *Training* – Vendor provides training to the TTB and other stakeholders, to ensure system operation is in accordance with vendor manuals and technical documentation.
- *Configuration Audit Support* – Vendor supports the TTB, TIOB CM Manager, and/or TSIF Test CM Lead, to conduct the configuration audit.
- *TSE Installation* – In coordination with the Contracting Officer's Representative, PMO, and TIOB, vendor supports onsite installation and integration.
- *Verification Support* – Vendor provides demonstrations to the TTB, and other stakeholders, for requirement for compliance verification.

- *System Maintenance* – Vendor performs corrective maintenance as needed or scheduled preventive maintenance.

4.2.9 QT Readiness Review

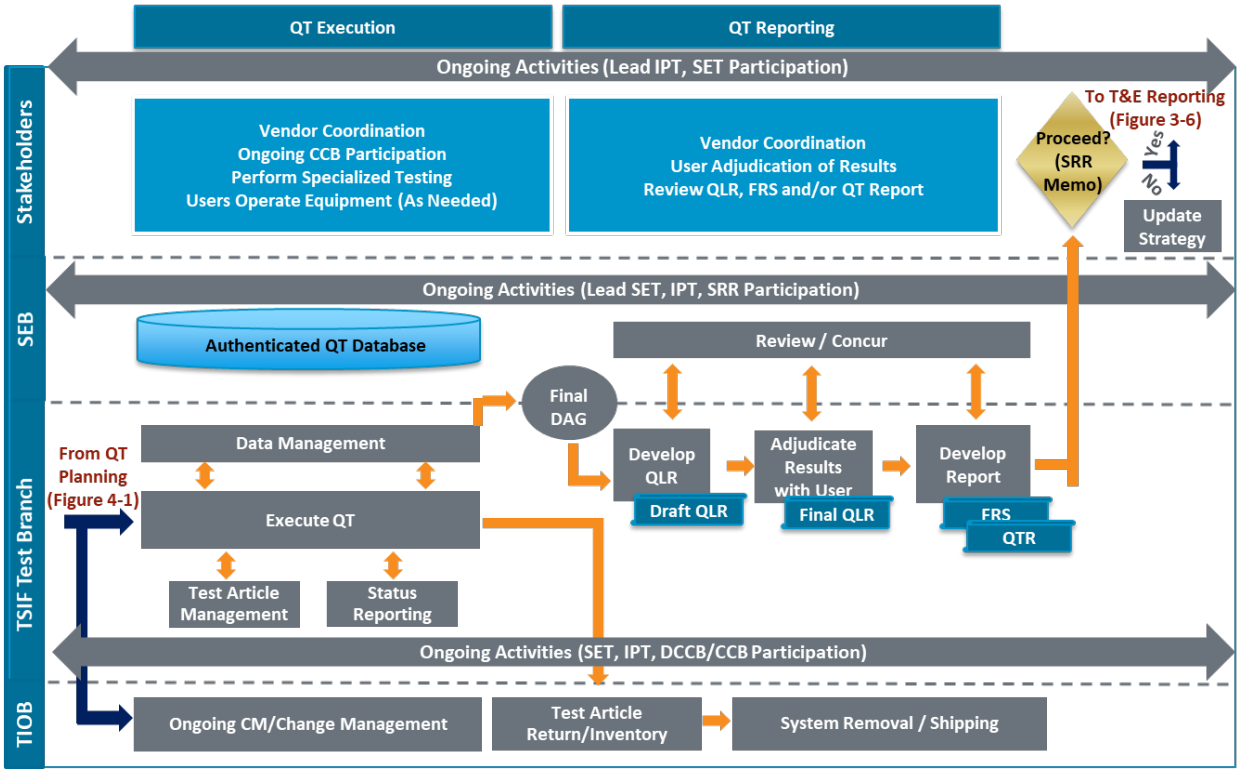
The QTRR is a forum to determine the status of all QT prerequisites and to obtain formal approval to enter test execution. The QTD is responsible for presenting the QTRR checklist and completion status for each readiness criteria to the forum. QTRR participation, at a minimum, includes the PMO Representative (and/or T&E Manager), System Evaluator, QTD, TTB Manager, and DOT&E Test Area Manager or designee, and is open for participation from other principal members of the SET and T&E IPT. The TTB Manager typically acts on behalf of the CAE as QTRR chair unless otherwise directed by the CAE.

During the QTRR, the QTD presents all planning activities demonstrate to the forum that the QT entrance criteria are met, allowing the TTB to support the successful conduct of the test. These criteria include test resource availability, safety, training, SUT readiness, and instrumentation availability. The QTD also demonstrates that T&E planning documentation, system baseline configuration, and data management processes have been adequately addressed by the TTB. The outcome of the QTRR is a unanimous determination by participating members that the QT is ready to begin. The QTRR chair provides the final determination in cases where consensus on next steps is not reached.

4.3 QT Execution and Reporting

During test execution, the TTB collects quantitative and qualitative data in accordance with the test scenarios in the QTP. Upon completion of testing, the TTB typically prepares either a QLR and QTR, or an FRS. Upon delivery of the QLR or FRS, the TTB holds a User Adjudication session, and the TTB documents the results of that meeting in a revision to the QT reports. **Figure 4-2** describes key activities taking place during QT execution and reporting.

Figure 4-2: QT Execution Process Flow



4.3.1 Test Execution

The TTB follows the test methods in each test scenario contained in the QTP, to collect the data required to fully analyze each requirement assigned to the TTB through the EF. The TTB may refer to the vendor-provided QDP documentation when resolving certain requirements (e.g., electrical and emissions regulatory safety requirements) as documented in the EF. The TTB will determine whether the SUT meets each requirement, and document these findings.

4.3.2 QT DAG

The DAG is a forum co-chaired by the QTD and System Evaluator, and consisting of other members of the T&E IPT. It convenes periodically during, and immediately after, test execution. Data authentication consists of a comprehensive review to ensure the data collected during test execution are sufficient to allow the TTB to determine compliance to the requirements. The DAG ensures the data are complete, accurate, consistent, and representative of SUT performance within the testing environment. The QTD conducts the DAG meeting to provide quality assurance of the collected data, not to review or adjudicate test results. The output of the DAG is authenticated results for use in data analysis and reporting.

The QTD and System Evaluator co-chair the DAG and serve as the final decision makers when authenticating data. DAG participants may not release data without the prior permission of a DAG co-chairs. **Table 4-2** lists the minimum required DAG personnel and their roles.

Table 4-2: QT DAG Personnel

Test Role	DAG Role
QTD	DAG Co-Chair
System Evaluator	DAG Co-Chair
TTB Manager (optional)	Attends DAG/Alternate Chair
QT Support Team Lead Engineer	Leads presentation of test data
QT Support Team Personnel	Provides details on collected data
PMO Representative	Provides technical context for requirements
User Representative	Provides operational context for requirements

At the DAG meeting, the TTB reviews the data collection methodology documented in each test scenario in the QTP, presents any limitations which occurred during testing that impacted this methodology or the collection of the data, and discusses how those limitations will affect the data and TTB's determination of requirements compliance. The members of the DAG will determine whether the TTB can use the data, including any limitations, for analysis and reporting. Any inquiries about the data are directed to the QTD, who either answers the question or conducts an investigation and provides the answer during the next DAG meeting.

The QTD considers all input and recommendations from the DAG to decide the most logical path for resolving each issue, and whether additional data collection is required to resolve them. If required, the QTD will coordinate with the PMO to determine whether changes are required to the scope, schedule, and/or funding.

4.3.3 Data Analysis and Reporting

The TTB compiles and analyzes authenticated test data with respect to requirement thresholds and any other success criteria from the QTP. In addition to computing results for each of the test scenarios, the TTB examines the data for trends that provides additional meaning and insight to the test results.

Critical to the analysis of QT results is the documentation of observations and additional findings, even if not directly associated to a requirement, that may have a profound impact in an operational environment. Analysts follow the guidance listed in the *Data Collection and Analysis Handbook,* dated January 24, 2023, when documenting results, to include leveraging hypothesis testing for detection requirements. The confidence level used is typically 90% when documenting results. The System Evaluator is a critical reviewer of the final test results to ensure the data accurately reflect the capabilities and deficiencies of the system.

The TTB prepares a QLR if required in the QTP. The QLR provides preliminary findings based on QT data, typically used as the primary reference during the user adjudication session of test findings, and is followed by a final QTR. The TTB develops the QLR upon completion of the

QT, with a delivery date of 15 business days after the final DAG meeting. The QTD gains concurrence from the System Evaluator, and final approval from the TTB Manager, prior to final delivery of the QLR.

The QTD delivers an FRS 15 business days after the final QT DAG meeting, or a QTR 45 business days after the final QT DAG meeting, based on the reporting requirements documented in the QTP and Program IMS. The QTD produces an FRS when the SET concludes that there is not a need for a QTR, and in cases where a formal, yet abbreviated document is required to meet schedule requirements.

The QTD delivers a Data Collection Activity Report (DCAR) for Data Collection Activities 45 business days after the final DAG meeting. The QTR, FRS, and DCAR describe system performance and limitations against requirements. The QTD provides these to the System Evaluator for use as an input during SER development and to the OTD to assist with OT planning. The System Evaluator provides concurrence/approval to the QTR and FRS.

The TTB Manager is the final approver of the QTR, FRS, and DCAR. The QTD is the final approver of the QLR. Using QT results and findings as an input, the PMO issues a System Readiness Review (SRR) memorandum confirming system readiness for OT. If QT and OT are conducted in parallel, there is no SRR memorandum required.

The TTB will record results, by requirement. This is the formal determination of SUT compliance with the requirements. When results are not adjudicated with the User and/or other Subject Matter Experts (SMEs), this met/not-met assessment in **Table 4-3** will be the final result. The TTB typically utilizes this approach only for Data Collection Activities.

Table 4-3: Determination of Compliance with Requirements

Compliance	Definition	Assessment
Not Met	Indicates sufficient test data to attest that the system has not met the requirement.	**Do not proceed**
Met	Indicates sufficient testing to attest to the ability of the system to meet the requirement with a high level of confidence.	**Proceed**
ID	Indicates Insufficient Data (ID) to form conclusions.	
NA	Indicates item was not applicable.	
NT	Indicates requirement was not tested.	

4.3.4 Results Adjudication

The QTD will transmit the QLR, with the initial results as indicated in **Table 4-3**, to the PMO, user representative, and other SET stakeholders. The QTD will then schedule a results adjudication session with minimum required attendance by the User Representative, System Evaluator, and PMO. The QTD will invite additional stakeholders as required. For example, if not-met requirements are related to cybersecurity, IT/IAD personnel may be invited to provide input to severity scores.

The stakeholders will provide feedback on the impact of each not-met requirement. The User Representative will provide the final severity score using the ratings listed in **Table 4-4**. The User Representative also determines or confirms workarounds to SUT limitations, and provides feedback on any additional findings or concerns. The QTD facilitates this meeting by presenting each not-met finding, providing technical details, and documenting final severity scores and accepted workarounds.

Table 4-4: QT Severity Ratings (Adjudicated)

Severity	Description
High	• Prevent the accomplishment of an operational and/or mission essential capability. • No work-around solution is available to lessen the operational impact. • Jeopardize safety or security in an unacceptable manner for operational use.
Medium	• Adversely affects the accomplishment of an operational and/or mission essential capability. • Can apply when a work-around solution is known and accepted by the User Representative that lessens the operational impact.
Low	• Results in a user/operator inconvenience or annoyance but does not affect a required operational or mission essential capability • A “nice to have” capability.
Accepted	• The user representative accepts the not-met finding as acceptable for normal operations.

Once the User Representative completes the assignment of severity scores, the PMO will make a determination of how to proceed in the qualification activity. The following lists two examples:

- The PMO accepts the risk of severity scores as listed and determines to proceed with the next activity in the SUT’s qualification process (e.g., OT).
- The PMO determines the vendor needs to address high severity deficiencies and adds a developmental remediation period to the IMS with a subsequent RQT.

The TTB typically releases a revision of the QLR or FRS as a final record of the User Representative’s adjudicated results and accepted workarounds. The QTR will also include this information.

4.3.5 Regression QT

If the User adjudication process identifies high severity non-compliances with functional requirements, or the SUT does not meet the entrance criteria for OT due to other technical issues, the PMO will typically task the vendor to provide remediation, in order to be allowed to continue through the Qualification Process. As part of re-entry, the TTB typically performs a formal RQT to determine the effect of any system configuration change made as part of this remediation, following the process described in section 3.8 of this guidebook.

Following an RQT, the TTB will produce an FRS documenting the test findings and repeat the User adjudication process, if required.

4.3.6 Test Article Management

The TIOB Test Article Group develops, acquires, and controls QT articles. During test execution, the TTB manages the inventory, use, and control of test articles and returns the articles to the TIOB Test Article Group on completion of test activities. The TTB ensures sensitive test articles are not visible to non-test team visitors (e.g., vendors, tours) to the test site. The TIOB Team maintains a current inventory of all articles available or in use.

4.3.7 Configuration Control During Test Execution

Configuration control, more appropriately termed "configuration change management," or simply "change management" in the ANSI/NIST EIA-649 C, Configuration Management Standard, is a highly valuable CM function and should be treated as a pillar of CM best practices. Configuration changes to an already established system baseline - during test execution activities – is strictly prohibited, unless authorized by PMO per an approved CR. The purpose of the configuration control function is to ensure that:

- Traceability is maintained for all proposed system changes.
- SUT performance during testing can be tied to a specific, well-documented system configuration.
- System baselines are managed/controlled at the appropriate level, and by the appropriate entity – i.e., RFD/engineering change proposal for procured/deployed systems (APM CCB), DEP for developmental systems (APM/TIOB CM Manager for systems undergoing a QT).
- Approved changes are limited or restricted to only specific system(s) defined in the effectivity section of the CR package.
- The integrity of the system baseline is maintained throughout the system lifecycle.

The TSA/APM CCB is responsible for evaluating and adjudicating hardware, software/firmware, configurable settings, or other system changes that may affect the approved product baseline of procured/deployed TSE – i.e., post contract award through RFDs (limited effectivity) and engineering change proposals (fleet wide effectivity). The TIOB CM Manager is responsible for managing changes that may affect the configuration baseline of developmental systems (the ATCB for TSIF TSE undergoing a QT). The ITA contributes to CR adjudication by evaluating how a proposed change could impact TSE functionality previous evaluation results for fielded systems, and the TTB places additional consideration to CRs that affect TSIF TSE installed in TSIF lab spaces.

As part of the overall configuration control process outlined above, the System Evaluator receives continual input from the Test Directors to determine whether any changes to system configuration require regression testing. The System Evaluator communicates impacts/risks to schedule and budget to the PMO prior to approval of any given change package. For TSIF TSE, the TIOB CM Manager, or assigned designee, is responsible for inspecting the affected system for compliance and correct incorporation of approved system changes to ensure that replaced CIs conform to the approved CR package, and integrity of the system ATCB is maintained. For

fielded systems, the QTD, or assigned designee, is responsible for witnessing/verifying compliance and correct incorporation of approved system changes at the TSIF.

4.3.8 Maintenance Activities

Maintenance activities during a QT event occur per the guidelines established in the QT TRN. Once the test event begins, the primary need for vendor onsite participation is preventive or corrective maintenance. Preventive maintenance activities are planned maintenance on the TSE often occurring at regular intervals (e.g., weekly). While some of these actions can be performed by the TTB, others require vendor involvement. TSA defines corrective maintenance as unanticipated requests for remediation due to an equipment malfunction.

Prior to test execution, vendors must coordinate corrective and preventive maintenance activities with the TIOB Test Area Lead and the QTD in the form of a schedule of activities as documented in the QT TRN. Prior to each maintenance activity, the vendor should coordinate with the TIOB Test Area Lead and QTD to coordinate the visit. The TTB and/or TIOB Test Area Lead monitors all preventive and corrective maintenance during the test event to ensure only the required maintenance is occurring. The TIOB Test Area Lead will document all actions performed by the service technician in a TSE Maintenance Checklist while the TTB records the maintenance actions in a TIR and system logbook as necessary.

4.3.9 Termination of QT Activities

A QT concludes once the TTB has completed and reported on all test scenarios documented in the QTP. Generally, the PMO and QTD support continuing the qualification process (e.g., entering an OT), if QT met the following criteria:

- No open issues rated High as defined in **Table 4-4**.
- Medium and Low issues do not significantly impede the operator's ability to perform mission-essential tasks.
- Configuration baseline established with no critical configuration management issues.
- All required test scenarios completed.

Certain conditions can create the need for early termination of QT activities. While the PMO's Qualification Management Plan will typically list programmatic reasons for early termination, other events could also cause the suspension of QT. These include the following:

- Discovery of a critical deficiency in the SUT, which creates a health or safety risk for test personnel.
- Limitations or failures of the SUT, which impede the data collection objectives documented in the QTP.
- Discovery of a system configuration discrepancy, such as an unapproved configuration item or system setting, which would invalidate collected data.
- A violation by the vendor of the restrictions listed in the QT TRN.

5.0 OPERATIONAL TESTING

Operational testing validates the extent to which candidate systems are Operationally Effective, Suitable, and Resilient in the operational environment. This phase of testing focuses on evaluating operational requirements from the ORD as defined by the User organization and serves as a realistic demonstration of a systems expected operational performance. Depending on the program and TES, TSA may hold an integrated OT event where requirements typically validated in a laboratory environment are instead validated in the operational environment.

5.1 OT Events Overview

The OTB performs OTs and OAs in support of an acquisition program TES. Due to threat intelligence, procedural development, and R&D, needs for operational data collection arise outside of a planned acquisition activity. Data collection in support of these needs are categorized as OUEs. **Table 5-1** lists the various types of test activities occurring in the operational environment and their purpose.

Table 5-1: Operational Testing Activities

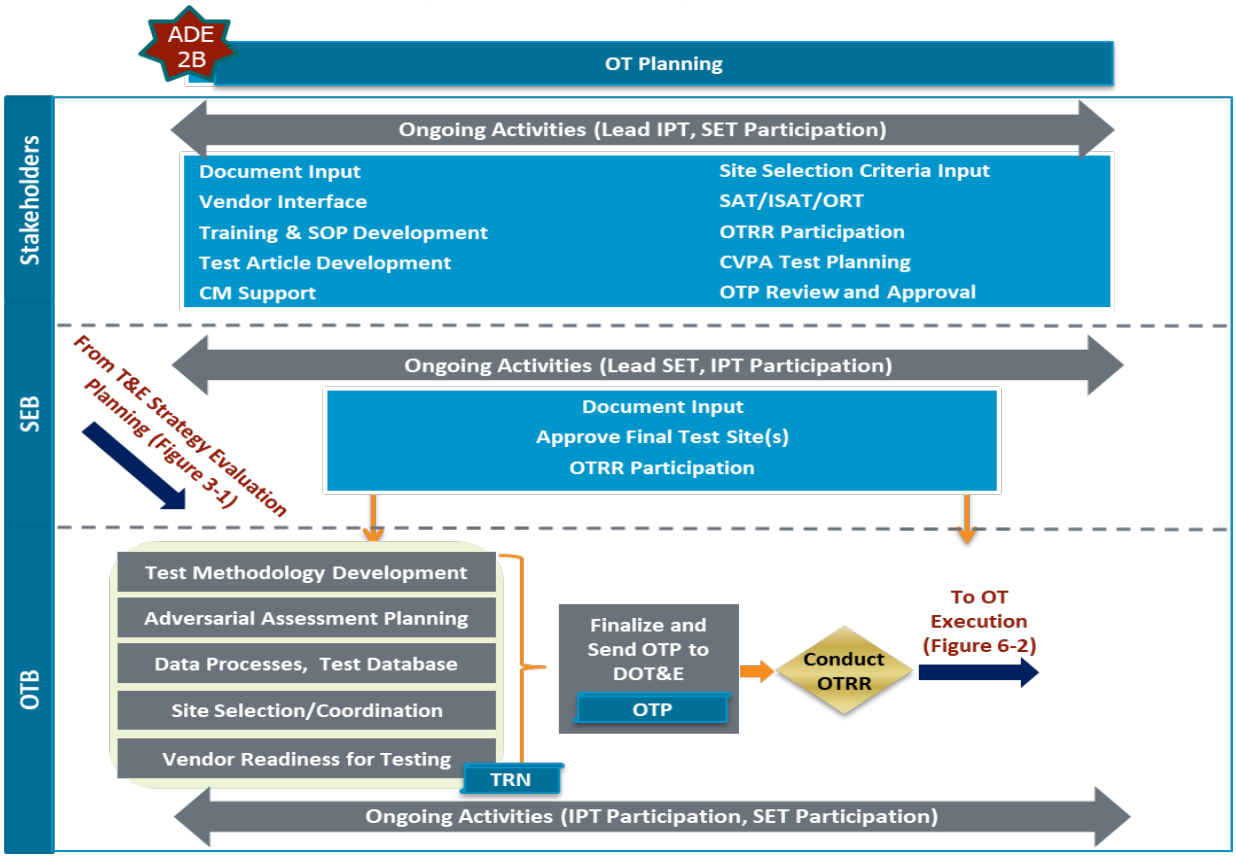
Test Event	Additional Detail/Decision Type	Plan	Report(s)
Initial Operational Test and Evaluation (IOT&E)	OTB conducts an IOT&E to inform an ADE-3 and evaluate a system's Operational Effectiveness, Suitability, and Resilience using typical, trained personnel in a realistic operational environment. The IOT&E is the initial OT event for a system.	OTP	QLR ERB SER
FOT&E	An FOT&E may be necessary to verify the resolution of issues discovered during an IOT&E or previous FOT&E. An FOT&E is also used to reevaluate the system when a vendor proposes changes to ensure that it continues to meet operational needs.	FOTP	QLR ERB SER or SER Redress
AA	An AA assesses the ability of the system to perform its mission in an operational environment while under cyber-attack. The AA is a subordinate activity to IOT&E and/or FOT&E and led by the ITA as a primary input to the System Evaluator's operational resilience rating in a SER.	OTP	AA Report SER
OA	A T&E activity conducted to determine readiness to begin initial production. An OA is conducted with trained users or SMEs using technology demonstrators, prototypes, mock-ups, or engineering development models to assess the system's risk to mission capability and future success during operational T&E. An ITA leads the OA effort which is conducted to support an ADE-2C decision or deployment of an initial capability into an operational environment.	OA Plan	OA Report

Test Event	Additional Detail/Decision Type	Plan	Report(s)
OUE	The OTB conducts an OUE on systems at any time and for a variety of purposes when collecting operational performance data is necessary. This can include R&D initiatives to identify system issues and capabilities. OUEs are streamlined and specific in nature whenever possible, and are adjustable to sponsor expectations. CM of OUE test units will be managed at the preference and direction of the sponsor organization (e.g., ITF) PM.	OUE Plan	OUE Report

5.2 OT Planning

The OTD, supported by the OTB Test Team, performs a number of planning activities to prepare for tests in the operational environment. Central to these planning activities is the development of an OTP, OA Plan, or OUE Plan. In general, the OTB Test Team may need to perform many of the same activities described in the following sections when planning for OTs, OAs, and OUEs with the exception that in some cases, the planning activity may not apply (or be less stringent) for OAs and OUEs. **Figure 5-1** describes the various activities taking place during test planning by the OTB, SEB, and other stakeholders in support of an OT event.

Figure 5-1: OT Planning Process Flow



5.2.1 Operational Test Plan

The OTD creates an OTP for test events in support of an acquisition program to align with the TEMP, SEP, and requirements allocated to OT as documented in the EF. The OTP describes the details of the test to include logistics, resources, test/data collection/ analysis methodologies, and test schedules. The following provides test plan documentation guidance for integrated test events:

- The OTD collaborates with any other assigned Test Director(s) participating in the integrated test event. For example, for in integrated OT/QT event, the OTD collaborates with the QTD to develop the integrated OTP.
- Using the EF, the Test Directors describe the test, data collection, and data analysis methodologies for verifying all integrated test requirements. Given requirements listed in the ORD and FRD correlate/overlap to some degree, the Test Directors must work to eliminate any duplication and unnecessary redundancy in the test plan. The test plan should represent the plan for a single integrated event rather than two separate plans under one cover.
- Test methodologies typically performed in a laboratory environment should be closely examined and modified as needed to account for verification in the operational environment. This may include utilizing SOC rather than controlled excursions using mock passengers and test team operators.
- For any measures requiring an excursion, the test plan should clearly describe the required tools and how these excursions will occur. Options may include executing the excursions when the system is not in use (e.g., after-hours) or taking the system offline during slow-traffic periods with the understanding that the offline hours can no longer be used for RMA purposes. In any case, the plan must be resourced appropriately, and logistics communicated with airport officials prior to the start of the integrated test event.

The OTD gains concurrence from the System Evaluator that the OTP will adequately support the evaluation and solicits OTP feedback from the SET. The OTD then routes the OTP for initial approval to the OTB Manager and SEB Manager, and final component-level approval by the Executive Director, ITA.

For major programs (non-delegated systems), upon Executive Director, ITA approval, the OTD routes the OTP for final approval by the DOT&E. The DOT&E approves the OTP within 60 days of submission, therefore, the OTD should ensure it is submitted with adequate time to not impact the start of the OT. The OTD should request approval from DOT&E if an expedited review is required to meet program milestones. Upon OTP final approval, the OTD archives the OTP into the OTB/SEB document library.

5.2.2 OA Plan and OUE Plan

The OTD creates an OA Plan to coordinate test execution activities prior to an OA and creates an OUE Plan in support of an OUE request from a sponsoring organization. The OA and OUE plans are similar to the OTP in that they contain all the necessary planning information for the test

event. The OTD gains approval from the System Evaluator that the OA Plan or OUE Plan will adequately support the data collection requirements needed to meet the test objectives of the activity. The OTD gains final OA Plan and OUE Plan approval from the OTB Manager.

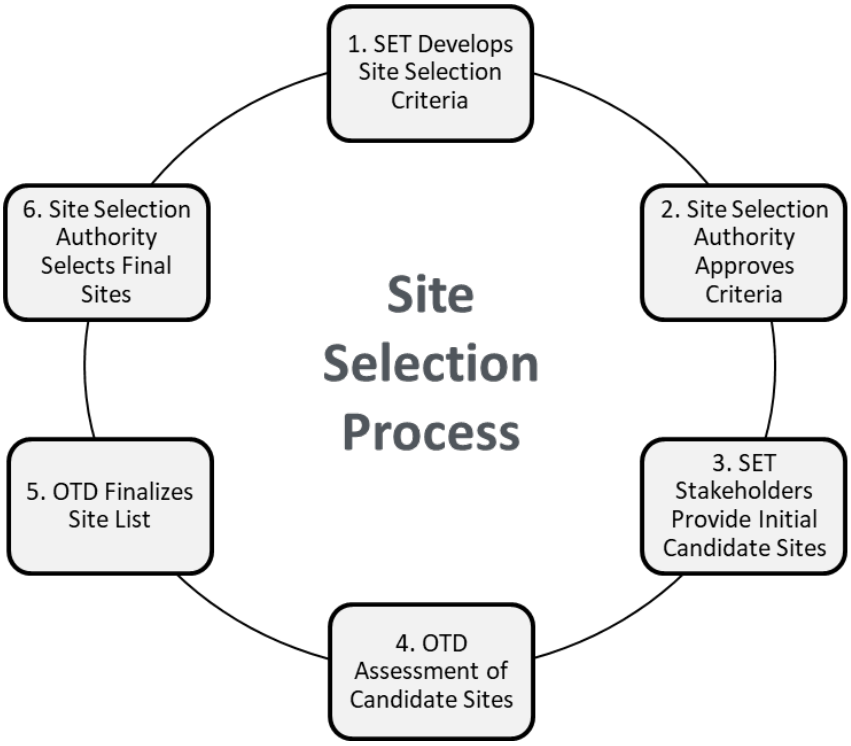
In cases where the System Evaluator intends to use the data collected during the OA or OUE as a primary data source in a SER, the final approval authority for the OA and OUE Plan is the Executive Director, ITA.

Upon OA Plan and/or OUE Plan final approval, the OTD archives the plan into the OTB/SEB document library.

5.2.3 Site Selection

The Site Selection Process may vary based on the system and testing requirements. The Site Selection Authority (SSA) will tailor each site selection to the test conditions required for the SUT, and the type of testing required (e.g., OUE, OT). The SSA for OT and OA events is the System Evaluator. The SSA for OUEs is the sponsoring/requesting organization. If data from the OUE event is intended to be used in support of a future acquisition evaluation, the System Evaluator is the SSA. **Figure 5-2** illustrates the typical site selection process.

Figure 5-2: Site Selection Process



5.2.3.1 SET Develops Site Selection Criteria

The System Evaluator identifies initial site selection criteria, documented in the TEMP. The SET develops additional site selection criteria, based on the operational requirements for the SUT. Site selection criteria may include such attributes as:

- Passenger and/or baggage demographics, or other operational factors representative of a typical deployment site if the system is procured.
- Ability to support test objectives to include required system configurations (e.g., baseline systems), overall test duration, volume, counts, and sample sizes.
- Geographically diverse sites to make sure the new system can operate the same way with different operator and passenger populations.
- Representative utilization rates, sufficient peak throughput rates, and ability to support required operating hours.
- Local ability to support testing (e.g., sufficient TSO manpower to support training and operations throughout the test duration).
- Test location does not present any significant safety concerns for operators or data collectors when executing necessary test activities.
- Compatible existing infrastructure (same vendor, dedicated power circuit, layout, etc.) and ease of installation of system upgrades and equipment.
- Airport badging process supports test schedules and planned costs.
- Available, secure storage for test equipment at a location near the SUT on airport grounds.
- Other airport activities do not negatively impact operations or user availability (e.g., training, blackout dates, construction, or other testing).

5.2.3.2 SSA Approves Criteria

The SSA approves the site selection criteria based on the test objectives and evaluation framework.

5.2.3.3 SET Stakeholders Provide Initial Candidate Sites

DSD and/or the User Representative provide candidate sites that potentially meet the key site selection criteria (e.g., infrastructure, throughput, daily operating time). SET stakeholders (e.g., PMO) may provide additional sites for consideration based on programmatic considerations (e.g., costs, schedule). These sites serve as initial locations for consideration.

The User Representative will make initial contact with the candidate sites to introduce the potential test event. The points of contact for the candidate sites are then provided to the OTD for further contact as needed during the site assessment discussed in the section below.

5.2.3.4 OTD Assessment of Candidate Sites

Once the SET has generated the candidate site list, the OTD will gather additional data as needed from sources such as the Enhanced Staffing Model, through a request to the User organization, or by communications with the candidate site points of contact. Through this coordination, the OTD can gather information surrounding test schedule, site availability, badging/access requirements, and whether the site has implemented any site-specific best practices to augment the approved TSA SOP (a potential disqualifying attribute). The OTD will use the compiled data to analyze/score the sites against the identified criteria in a Site Selection Worksheet resulting in a best qualified site list. A Site Selection Worksheet template is available in the OTB/SEB template library.

If the assessment of site selection criteria requires a site survey, the OTD will coordinate the site survey with the site POC. The site survey can be beneficial for site selection criteria surrounding TI testing, safety, checkpoint/checked baggage area physical layout, space considerations, and other similar aspects of the test. In preparation for the site survey, the OTD will review the site selection criteria and prepare a site survey checklist. This checklist will provide the various items requiring inspection by the OTD during the site visit. For example, the checklist would ensure adequate space and security is available for test bag storage, data collectors can safely and discreetly maneuver test bags to insertion points, accessible network ports for tests requiring system connectivity to a network, and adequate space exists such that data collectors can position themselves to not interrupt screening operations while collecting data.

5.2.3.5 OTD Finalizes Site List

The OTD updates the Site Selection Worksheet based on additional information gained during the site survey, prioritizes the sites, and provides it to the SET for feedback. The SET reviews the candidate site list and provides feedback to the OTD to inform the site ratings.

5.2.3.6 SSA Selects Final Sites

The System Evaluator selects the final test site(s) and the test location (e.g., checkpoint, lanes, bag zones) within those sites. The OTD documents the sites selected in the OTP as the final record and includes the rationale for the selected sites. At a minimum, the rationale includes the site's characteristics when compared to site selection criteria. The OTD may also include the site selection matrix and any other supporting information as an appendix.

5.2.4 Test Site Coordination and In-Briefs

The OTB Test Team coordinates regularly with the test sites from site selection through the completion of the test event. Coordination items generally include tester badging, test dates, and the status of the test. The OTD is responsible for providing the airport FSD management team with an in-brief explaining the roles and responsibilities throughout the test, data being collected, and anything else that should be expected. The session also serves as a forum for resolving any remaining questions and issues prior to the start of testing. The OTD is also responsible for coordinating a Law Enforcement Officer (LEO) in-brief (virtual or in-person) prior to the start of

a TI testing. The LEO in-brief should discuss the frequency of planned TI testing as well as actions to be taken to terminate the trial without issue.

5.2.5 Establishing Baseline Capability

As documented in the OTP, the OTB Test Team may perform baseline data collection prior to the OT. The objective of this activity is to determine the performance capability of current fielded systems for comparison purposes. Baseline data collection should only occur if required to verify an ORD or FRD requirement or when requested by the PMO. If these conditions are met, the System Evaluator should review existing data from past test events for potential use to satisfy the baseline data collection need. When possible, the OTB Test Team should perform baseline data collection at the same sites and locations (e.g., terminal, checkpoint) of the system that will be undergoing the OT. Baseline data collection planning is typically included in the OTP. The System Evaluator may use the data from baseline data collection as a reference in the SER.

5.2.6 Test Team Preparation and Training

The OTD and OTB Test Team ensure all data collection tools (e.g., data input forms) are developed in alignment with OTP methodologies and loaded onto appropriate instrumentation if applicable. The OTB Test Team develops training materials and provides the training to the onsite data collection team prior to traveling to the test site. If resources allow, the OTB Test Team, or a portion of the test team, should participate in a SUT demonstration and hands-on training event at the TSIF to ensure familiarity with the system and test methodology once the data collection period begins. A TSIF training event is particularly useful in circumstances where the program schedule has allocated a short duration for burn-in and/or when the SUT is new to the transportation security environment. OTB Test Team feedback from this training event can lead to revisions to data collection form design and utility prior to the beginning of burn-in.

5.2.7 OT TRN

The OT TRN describes the ground rules for vendor presence and participation during an OT event. The OTD will coordinate the OT TRN through the PMO Contracting Officer's Representative and will transmit the OT TRN to the vendor prior to the beginning of data collection. The vendor signs the OT TRN, affirming readiness of their system(s) for testing and their understanding of test protocols.

The OT TRN includes the procedures for a vendor to gain access to the TSE prior-to and during the test. There are several activities at the test site where a vendor's presence may be required. The vendor may be authorized to support any of the following activities:

- *Training*: Vendor onsite with local TSA airport teams to provide TSE training.
- *Configuration Audit Support*: Vendor onsite with test teams to support the configuration audit.
- *TSE Installation*: Vendor onsite to install the system in coordination with the DSD and PMO.

- *Site Acceptance Test (SAT)/Operational Readiness Test (ORT)/Integrated SAT (ISAT)*: Vendor onsite to support the AT Team-led SAT/ORT/ISAT.

Once the test begins, the primary need for vendor onsite participation is preventive and corrective maintenance. Vendors must coordinate preventive maintenance activities with the OTD prior to the test. Preventive maintenance activities should be performed prior to, or after, the system operational window for a given day. Prior to each scheduled preventive maintenance activity, the vendor should coordinate with the OTB Test Team to gain access to the system. TSA will notify the vendor through the established maintenance concept when TSA requires corrective maintenance. The OTB Test Team must monitor all preventive maintenance and corrective maintenance during the OT. The OT TRN explains to the vendor the following test protocols and restrictions.

- A vendor is not authorized to access the TSE without prior coordination with the OTD or the OTB Test Team Site Lead.
- A vendor must not change their typical maintenance protocol (e.g., increasing the number of maintenance personnel at a test site) to appear more responsive during the test period.
- During maintenance activities, the OTB Test Team monitors to ensure only the required maintenance is performed. It is appropriate for the OTB Test Team to question the technician as to the actions being taken to ensure the TIR is complete. The OTB Test Team documents any attempt to review system logs, change system configuration, or update system files.
- The System Evaluator must approve any release of test results and observations outside of DAG meetings. OTB Test Team members are not authorized to give test status reports, system performance results, FDRS data, etc., to vendors or others.
- At no time will vendor conversations with the OTB Test Team be construed as direction from the Government.
- Vendors are not authorized to contact or interrogate TSOs at any time during the test period.
- No vendor photography/videos may be taken of the SUT.

5.2.8 Verifying the System Configuration Prior to Test Execution

After the system has been installed and integrated in the operational environment, the AT Team performs a configuration audit against the MCIL as part of its ISAT/SAT/ORT activity and will perform any additional configuration verification (e.g., configurable settings) if documented in the submitted AT TRN. The AT Team provides audit results to the OTD and PMO, to include any MCIL discrepancies. The OTD and PMO will work with the vendor to resolve any discrepancies in order to ensure the record test configuration matches the system configuration from QT.

5.2.9 Configuration Control During Test Execution

Please refer to Section 4.3.7 for specific process guidance with respect to configuration control throughout test execution.

5.2.10 Operational Test Readiness Review

The OTD leads the OTRR, performed as a burn-in entry gate to ensure a system, and supporting procedures, are ready for data collection in the operational environment. The T&E Team is represented at the OTRR by the Executive Director, ITA, the OTB and SEB Managers, the OTD, the System Evaluator, and other test entity stakeholders as required. The following lists the voting members for major programs.

- *Major programs (non-delegated systems)*: User Representative; Lead Technical Authority as defined in the *DHS Technical Review Guide*; PMO Representative; AAD Representative; System Evaluator; OTB Manager; Executive Director, ITA; Executive Director, PEO; and the DOT&E with final approval belonging to the CAE.
- *Major programs (delegated systems) and major programs (post-FOC delivery)*: User Representative, PMO Representative, System Evaluator, and the OTB Manager with final approval belonging to the Executive Director, ITA and Executive Director, PEO.

OTRR voting members may delegate their vote when necessary. OTRR approval represents an approval to enter burn-in. At the completion of burn-in, the OTD prepares an STN email as discussed in Section 5.2.10.3.

5.2.10.1 OTRR Checklist

Prior to the OTRR, the OTD should ensure the SET has reviewed the OTRR Checklist and all items can be discussed with sufficient information to allow the OTRR Chair to make a determination. Each checklist item will have a color rating defined as follows:

- *Green*: Action completed.
- *Yellow*: Not started or incomplete; expected completion by the start of testing.
- *Red*: Not started or incomplete; a significant risk exists to completion by the start of testing.
- *Gray*: Item is not required for the test activity.

All items should be in green status prior to the OTRR or in yellow status if item completion is not required for burn-in to commence. If green status is not possible due to extenuating circumstances, the OTB Manager may approve the OTD to continue forward with scheduling the OTRR. The end product of any OTRR may also include required changes to ensure successful test execution, or a delay or cancellation of the OT.

5.2.10.2 OTRR Criteria

OTRR entrance criteria may include the following; however, criteria are subject to change:

- OTP approved.
- VV&A completed of any necessary test articles and documentation produced.
- Test resources, including equipment, personnel, and instrumentation, are in place.
- Any required prior testing (e.g., CERT, QT) completed with favorable results as adjudicated by the User Representative. The PM should document satisfactory results of prior testing in the form of an SRR. This item is not required in circumstances where OT is scheduled to occur in parallel to prior test activities.
- SUT configuration documented and frozen.
- Integration and installation completed and validated (SAT, ORT, or ISAT as applicable).
- Site coordination completed to include site visits and FSD management team in-brief.
- System operator and test personnel training completed or sufficient to begin burn-in with a plan for completion by the start of record testing.
- Training documentation, operator and maintenance manuals, and any required account and password information for system access provided to operators and the test team (if necessary).
- CONOPs and SOP for all modes of operation approved.
- Privacy Impact Assessment completed.
- Maintenance concept defined and communicated to all relevant parties.

5.2.10.3 Start of Testing Notification

On, or prior to, the last day of burn-in, the OTD sends an STN email to all OTRR parties to confirm that conditions are favorable (i.e., all items are in *Green* status) and declaring the system ready for the start of record test. In the event the system is not ready to enter record test, the OTD will notify OTRR parties as soon as possible as to the areas of concern and recommended action. Recommended actions include either extending the burn-in duration or suspending the test activity to a later date. In these instances, the OTD should coordinate the recommended action with the PM prior to issuing any communications concerning the record test period start date.

Prior to issuing the STN, the OTD attests to the following:

- System performance is stable. If indications during burn-in are that the system is likely to not achieve satisfactory performance during the OT, the OTD should notify the PM. The PM may decide to assume the performance risk and authorize the OT to commence.
- Sufficient users trained and operating the system as intended for all scheduled test operating hours.
- OTB Test Team data collection processes are viable, stable, and do not interfere with operations.
- Completed TI planning, to include LEO in-brief and TI site visit.

- All TI test articles received and stored at the site.

5.2.10.4 TRRs for AAs, OAs, and OUEs.

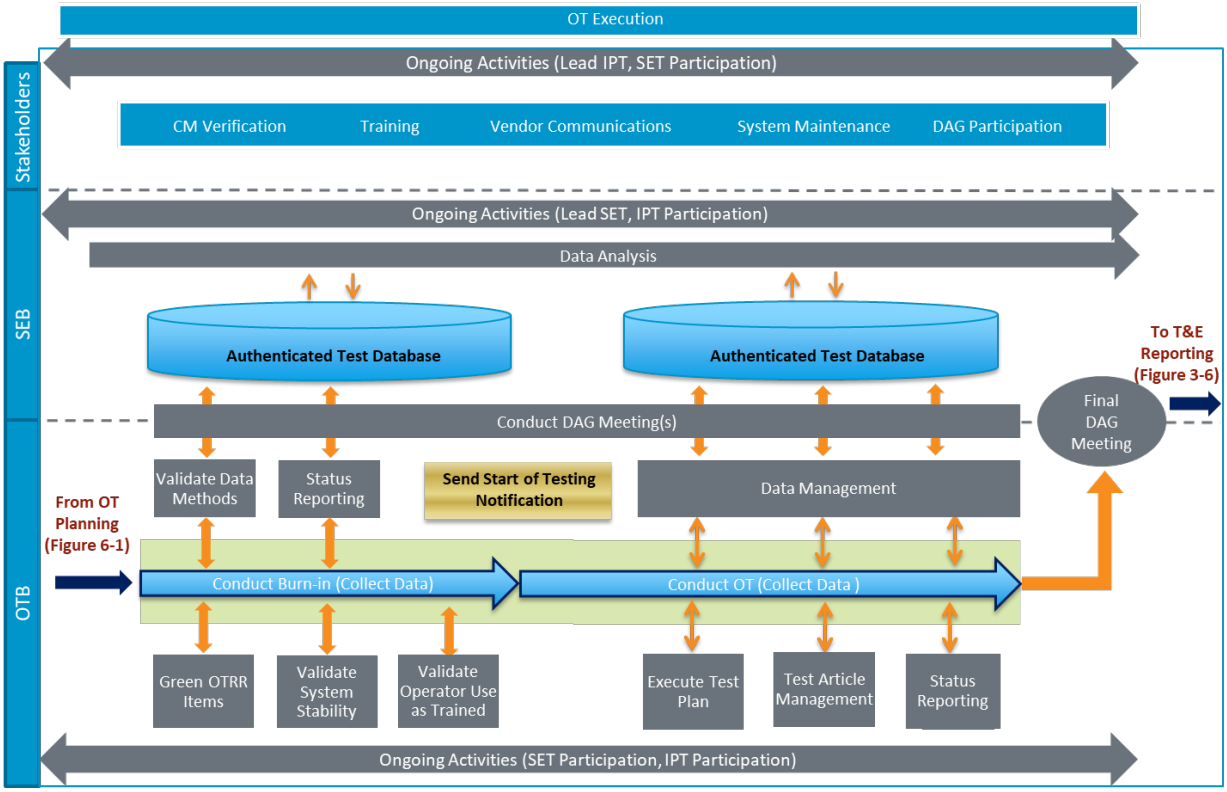
The AA (described further in Appendix D) test activity within the overarching OT requires a dedicated set of Test Readiness Review (TRR) materials as the readiness criteria will differ from the criteria required for field data collection. If start dates coincide, the AA TRR and OTRR can be conducted in the same session where the OTD presents the readiness slides for each sequentially. The chair and voting members for an AA TRR will be identical to the OTRR with the addition of the IAD Representative and corresponding QTD if the AA activity is taking place at the TSIF.

Similar to an OTRR, the OTD schedules a TRR prior to burn-in in support of an OA or OUE. The TRR participants should include, at a minimum, the OTD, System Evaluator, and User Representative, and PM staff should also be in attendance. For OUEs, the sponsoring organization (e.g., RCA, PMO) should attend. The OTB Manager is the TRR Chair for OAs and OUEs.

5.3 Burn-In and Test Execution

During burn-in and test execution, the OTB Test Team collects data in accordance with the test plan while operators use the system in accordance with the approved SOP. **Figure 5-3** illustrates the various activities taking place during test execution in support of an acquisition program OT.

Figure 5-3: OT Execution Process Flow



5.3.1 Burn-In

Immediately following OTRR Chair approval, a system enters OT burn-in. Operators training and burn-in typically commence as soon as SUT completes installation and passes AT. During this period, operators continue to use the system with the approved SOP to gain familiarity with the SUT and associated procedures. OT burn-in provides an opportunity for the OTB Test Team to validate data collection methodologies and forms. As Users become familiar with the system, OTB Test Team data collection processes stabilize, enabling data integrity when record testing begins. Finally, burn-in provides the system an opportunity to demonstrate stable operational performance. The burn-in period is normally scheduled from three to 10 days depending on the complexity of the system. However, burn-in is event driven, meaning it will last as long as required to meet its purpose. If a system (technology or procedures) experiences considerable issues in the operational environment, a decision not to proceed to record testing may occur upon confirmation by the PM.

5.3.2 Test Execution and Data Collection

Once record testing begins, the OTB Test Team executes test procedures as documented in the test plan. The OTB Test Team collects data in a non-interference manner, however, they should intervene (notify the TSO) if observing a procedural or system deficiency that introduces a possible security breach. The OTB Test Team must document any intervention as a test incident and report the intervention in the next daily status report, ensuring the PMO and User Representative are copied.

OTB uses a TIR to capture essential data on test incidents as they occur. All system failures should have an associated TIR. It contains at a minimum, a description of the test incident, any associated downtime, and corrective action. The System Evaluator uses these data to resolve RMA measures in the SER. The OTB Test Team stores all TIRs in the test database and reviews them regularly during the DAG for authentication. The OTB Test Team may also record TIRs not associated with system failures (e.g., improper vendor access of TSE, checkpoint lane closure, security breach, etc.)

5.3.3 Early Termination of Operational Testing

In addition to the restrictions listed in the OT TRN, other factors could also cause the suspension of the OT event. These include the following:

- A critical safety deficiency arises.
- TSE disrupts, impedes, or degrades operations to the point where airport officials and/or the User Representative requests SUT removal.
- Operator or technical procedures are not adequate, disrupt, or delay testing such that the objectives of the test plan cannot be met.
- Vendor inappropriately interferes with the test or system configuration.
- The OTB Test Team discovers an unapproved system configuration discrepancy.

The specific actions to be taken upon early test termination are documented in the test plan. The following is an example of the actions to be taken.

- Local TSA informs OTB Test Team Site Lead of possible infraction.
- In cases of emergency or safety incidents, the OTD may suspend the event and/or system operation while the rest of this process is followed. In such events, local TSA may suspend lane operations and immediately notify the site lead and/or OTD.
- The OTB Test Team Site Lead immediately notifies the OTD and OTB Test Team chain of command, followed by a written sequence of events to the OTD within 2 hours of notification. For non-emergency or safety incidents, the OTB Test Team continues observations and reporting until receipt of further guidance from OTD.
- The OTD notifies the T&E Manager, System Evaluator, PM, and OTB and SEB Branch Managers of the infraction.
- In case of infraction related to system performance, the OTB Test Team Analyst provides the OTD and System Evaluator with a preliminary data report within 24 hours of OTD notification.
- The OTD determines the course of action and notifies the PM to gain concurrence. The OTD provides direction to the OTB Test Team and informs Local TSA. The PM determines if events cause a delay and update timelines.

5.3.4 Test Closeout and Site Restoration

Upon completion of the OT, the PMO works with the User organization, DSD, and airport authorities to remove test instrumentation and systems, to restore the normal screening TSE layout in a timely fashion, and to ensure minimum impact to local operations. In some cases, a joint decision is made to leave the test TSE at the site, in which case these site restoration activities will not take place. Upon request, airport officials may request an OT closeout briefing. The OTD should include in this briefing, a high-level overview of test activities during the period and any pertinent site-specific topics. There will be no detailed test results released until formally reported in an approved SER.

5.4 TI Testing

5.4.1 TI Test Planning

The OTB conducts TI testing when required in the OTP to assess whether the system (inclusive of operator and procedures) is effective at detecting threats. Proper planning ensures test integrity, risks are minimized, and that the required numbers of samples are collected.

The TIOB, or other ITA-designated entity (e.g., TSL/IT&E), develops the threat test articles in support of TI testing. Unless otherwise specified in the OTP, the test articles should represent the spectrum of possible system threats (e.g., various detection tiers, PIs). Any test bags used for TI testing should have contents (clutter) that represent the current SOC. The System Evaluator

ensures the User Representative validates the threat articles through a threat validation memorandum prior to concurring with the OTP.

The System Evaluator and OTD work with the OTB Test Team to create the TI test methodology, design of experiments, and data collection forms. The scenarios listed in the design of experiments are typically staggered to ensure variability in times and the frequency of scenarios per day. The OTP should discuss the test and analysis methodology to include number of trials, types of trials, durations, and how a met/not-met determination will be reached. This should include comparison to thresholds, baseline system performance, or User adjudication post-test to determine whether the results are acceptable.

Additional critical planning elements include OTB Test Team training materials, memorandums to be used for ending trials, and test termination protocols.

5.4.2 TI Execution

A Threat Inject Carrier (TIC) is generally required for checkpoint-based TI testing to execute the scenarios in accordance with the OTP and TI training. If no detection is made, the nature of the test is not revealed so as not to compromise the TIC's identity. If a detection is made, the OTB Test Team follows the procedures defined in the "Terminating the Test" section of training.

During test execution, it is critical that the OTB Test Team take precautions to not compromise the TIC and test articles. The following components should not be revealed to local airport staff and operators prior to and during the test period to maintain test integrity:

- Test article storage location
- TIC identity
- Scenario details and schedule

When executing checkpoint TI trials, anonymity of TICs is paramount to test integrity. If a TIC's identity is revealed, TSOs may modify their typical screening behavior. The TIC should be prepared to answer any common questions asked by TSOs as a typical passenger would without becoming combative. The TIC should always remain calm, not drawing attention to the threat object even when discovered. Minimal attention during a detection increases the likelihood of executing the remaining trials for that TIC and/or test article.

5.4.3 Working with TI Data

The OTB Test Team should safeguard TI data appropriately per assigned classification to prevent vulnerability data from being released.

During test execution, the OTB Test Team collects TI results and observations each day and transmits them as appropriate for analysis and reporting. TSA considers the TI data collected daily as Sensitive Security Information or SSI. In addition to SSI guidelines, the OTB Test Team should take precautions when collecting the results of the test runs, encoding results whenever possible. Analysts should transmit the data to the Homeland Security Domain Network regularly and delete any original files. Once compiled, the analysts classify the data as SECRET on the

Homeland Security Domain Network and handle it in accordance with the approved DHS TSA Security Classification Guide as signed by the TSA Administrator.

5.4.4 Test Article Security

Test articles used during TI testing must be securely stored on airport grounds (unless otherwise approved by the TIOB Manager) and in a secure location under OTB Test Team control at all times. When shipping test articles, only a traceable shipping method from a reputable carrier must be used. Test bags and threat articles (e.g., simulants, PIs) must be shipped from the TSIF (or other test article manufacturing location as approved by the TIOB Manager) with a DD1149 form completed to document threat article chain of custody. The OTB Test Team provides the TIOB Manager with shipment details so that TIOB personnel have the opportunity to witness the bags being palletized, shrink wrapped, and placed on the shipping vehicle. They must also receive a signed bill of lading detailing the shipment.

5.5 OT Data Authentication

The mission of the DAG is to periodically review and authenticate data collected during the test event. Data authentication consists of a comprehensive review to ensure the data are complete, accurate, consistent, and representative of system performance within the operational environment. The DAG also ascertains whether the T&E Team properly collected and reduced the data. Generally, the DAG will review all data collected for a set period of time. On a case-by-case basis, the OTD may schedule a DAG meeting to focus on a specific set of data (e.g., RMA scoring conference reviews TIRs). The output of the DAG meeting is an authenticated database used for data analysis and reporting. DAG meetings to review TI data are held within an approved location for classified discussions.

5.5.1 OT DAG Personnel

The OTD will conduct DAG meetings with the System Evaluator and other stakeholders during the test period. The System Evaluator chairs the DAG and is the final decision maker when authenticating data. The DAG is composed of a multi-disciplined team of representatives from the SEB, OTB, User Representative, and PMO. The OTB Test Team provides additional information regarding the data collected to support discussions. DAG participants may not release data, nor disseminate test results to any parties not invited to the DAG, without the prior permission of the System Evaluator. **Table 5-2** lists the minimum required DAG personnel and their roles.

Table 5-2: OT DAG Personnel

Test Role	DAG Role
System Evaluator	DAG Chair
OTD	Alternate DAG Chair. Provides details on collected data.
Lead Analyst	Presents data and records final DAG score
User Representative	Participant

PMO Representative	Participant

5.5.2 DAG Scoring Criteria

The DAG assigns scores to the data based upon information presented, discussions, investigation results, and system knowledge. The OTB Test Team records the authentication scores in the test database after the DAG meetings to ensure authenticated data are used during final analysis and reporting. There are four authentication scores that the DAG can assign to each record:

- *Authenticated* data are complete, accurately represent operations, and can be used in its entirety by the System Evaluator during final analysis and reporting.
- *Investigation* data are those records that require further research by the OTB Test Team before the DAG can score the data. The OTB Test Team must resubmit these records to the DAG when the investigation is complete for scoring.
- *Limited Use* data are those records that contain partially authenticated data elements and can be used for certain analyses, but not others. For example, the results of a scan are available for accuracy assessment but the timing for the sample may be incomplete and unable to be used for computing a timing metric. The Lead Analyst should clearly denote the authenticated and not-authenticated fields/elements of the record.
- *No Test* data are those records the DAG considered non-representative, incomplete, or erroneous and not used for analysis.

5.5.3 DAG Procedures

Prior to the DAG meeting, the OTB Test Team sends all DAG participants a data file consisting of the data to review for the DAG session. The OTB Test Team instructs DAG participants to review the data prior to the meeting to expedite the review.

To minimize the chances of data release prior to analysis, the DAG Chair should document DAG ground rules in the initial release of the DAG file and then verbally during the initial DAG session, and at following DAG sessions as needed. Specifically, the DAG Chair should caveat that the data are preliminary and have not been analyzed per approved methodologies. Stakeholder attempts to analyze these data sets and share results could result in erroneous findings and conclusions.

At the DAG meeting, the OTD and Lead Analyst presents the data file to include all data collected since the previous DAG data cutoff and all records previously marked as *Investigation*. The Lead Analyst also recommends a score based on pre-DAG data reduction. The DAG reviews the records and confirms or recommends an alternate score to the DAG Chair. The DAG Chair assigns the final DAG score. Any inquiries about the data records are directed to the OTD, Lead Analyst, and support team members, who may need to conduct an investigation and provide the answers during the next DAG meeting.

5.6 OT Event Reporting

5.6.1 OT QLR

The System Evaluator prepares an OT and/or OA QLR on a case-by-case basis as documented in the program IMS, OA Plan, and/or OTP, when information is required to understand the risk of proceeding to OT (OA QLR) or prior to a final SER (OT QLR). The QLR provides preliminary findings based on OT/OA data. The data used to compute these results may be preliminary. Therefore, prior to distribution, the System Evaluator ensures the QLR contains appropriate disclaimers, cautioning against its use for making key acquisition decisions.

When required, the System Evaluator delivers the QLR approximately 10 calendar days after the final DAG meeting. The System Evaluator gains concurrence from the OTB Manager prior to final OT QLR approval by the SEB Manager.

5.6.2 OT ERB

For major programs (non-delegated systems), the OTD develops and delivers an ERB to DOT&E within 30 calendar days of the last day of OT. The scope of the ERB is for OT only and does not include any information concerning QT or other data sources. The ERB includes unexpected test limitations that could impact the evaluation, deviations from the approved OTP, and any major incidents encountered during OT. The OTD should include the number of samples collected for each measure and compare quantity to the planned sample size. The ERB does not make conclusions nor does it include any trends or results.

For major programs (non-delegated systems), the OTD gains ERB concurrence from the SEB and OTB Managers, and final approval by the Executive Director, ITA prior to delivery to DOT&E. An ERB is not required for non-major programs, major programs (delegated systems), and major programs (post-FOC delivery).

5.6.3 OA Report

When an OA is conducted, the System Evaluator develops an OA Report describing system performance against the test objectives specified in the OA Plan. Upon prior coordination between the PMO and System Evaluator, a QLR may substitute for an OA Report to meet program IMS milestones. The System Evaluator should not present any formal determination of Operational Effectiveness, Suitability, and Resilience in an OA Report. Given the data collected in an OA provides an indication of system readiness to proceed to an OT, the System Evaluator should clearly describe system capabilities and limitations to ensure the PMO understands the risk of proceeding to an OT.

The System Evaluator delivers a signed OA Report within 45 calendar days after the final DAG meeting. The System Evaluator adjudicates SET feedback prior to finalizing the OAR. The System Evaluator sends OA Reports to the OTB Manager for initial approval and to the SEB Manager for final approval.

5.6.4 OUE Report

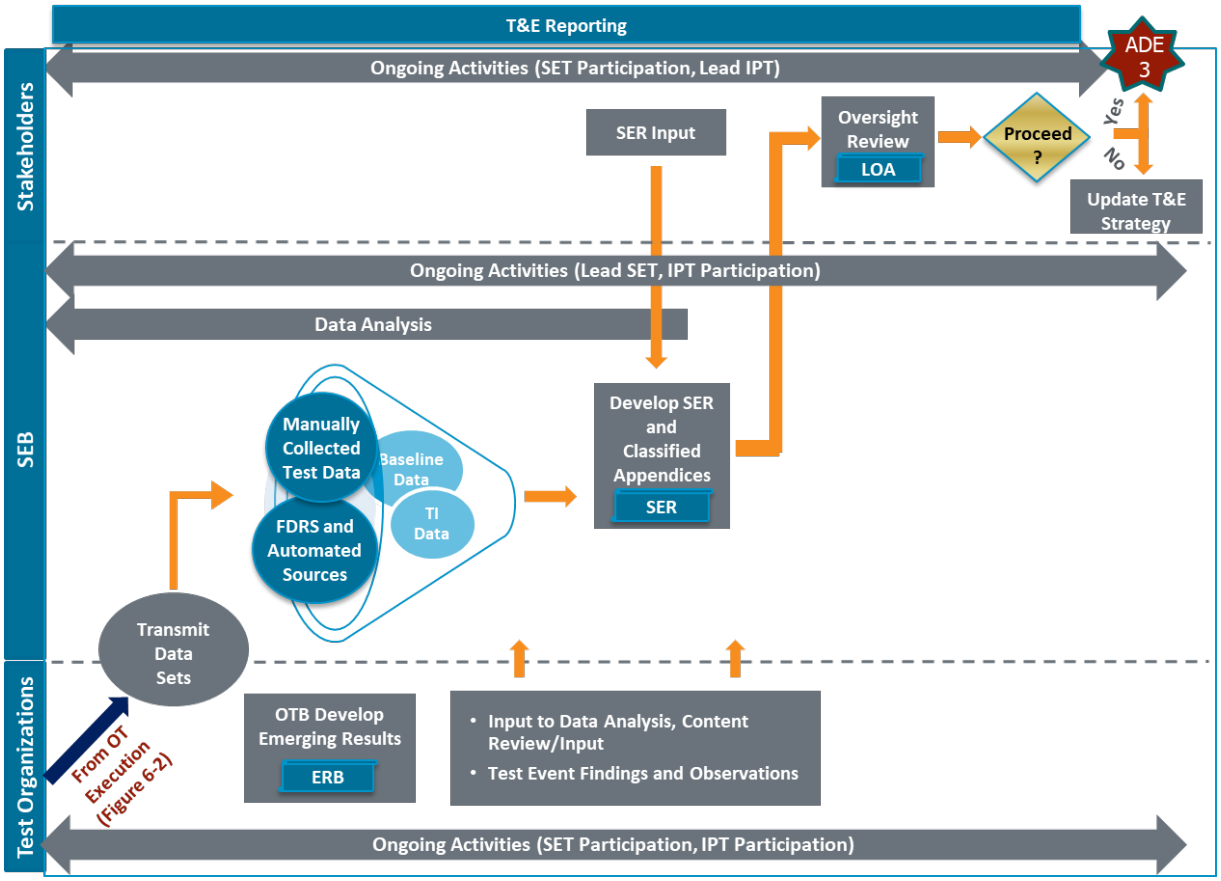
The OUE Report is the System Evaluator-prepared final report supporting OUEs. These reports provide system performance against the measures described in the OUE Plan. These reports do not include an Operational Effectiveness, Suitability, or Resilience rating and are tailorable in structure and content to ensure the information presented satisfies the objectives in the OUE Plan and meet the expectations of the OUE sponsor. The System Evaluator sends OUE Reports to the OTB Manager for initial approval and to the SEB Manager for final approval.

Upon OUE Report final approval, the System Evaluator archives the OUE Report into the OTB/SEB document library.

6.0 SYSTEM EVALUATION REPORT

Figure 6-1 illustrates the process for incorporating test event results, and developing evaluation level reports in support of an acquisition decision.

Figure 6-1: Evaluation Reporting Process Flow



6.1.1 Test Event Reporting in Support of the SER

Once test events have concluded, the appropriate Test Director sends the final data set, test findings, and any report created to the System Evaluator as an input to the SER. These reports include the CERT Report, QT Report, and AA Report.

6.1.2 SER Development

The System Evaluator delivers a signed SER no later than 45 calendar days after the final DAG meeting and 45 calendar days prior to any scheduled ARB unless an alternative agreement has been reached with the PMO and, for major programs (non-delegated systems), DOT&E. This allows DOT&E sufficient time for their LOA to be issued prior to the ARB. The SER (referred to as an "OT&E Report" in DHS T&E Directive 026-06) provides an independent evaluation of a system's Operational Effectiveness, Suitability, and Resilience and informs decision makers in

support of an ADE-3 full rate production decision. SER results are corroborated using data from all credible data sources. The SER addresses and answers the COIs, COICs, KPPs, and additional evaluation focus areas as described in the TEMP. When addressing these areas, analysts generally leverage hypothesis testing. The confidence level used is typically 90%. The confidence level used for assessing RMA measures is typically 80%. Statistical methodologies and best practices used in data analysis are described in the Data Collection and Analysis Handbook.

A core element of the SER is the System Evaluator's recommendations to the PMO and other stakeholder offices. These recommendations are summarized at the conclusion of the SER, listed by evaluation category (i.e., Effectiveness, Suitability, Resilience), and assigned to a measure from the SER. The measure alignment provides the reviewer with a reference for quickly navigating to the appropriate section of the SER for a better understanding of the basis for the recommendation. Further, each recommendation should be grouped in one of two tables per evaluation area (e.g., Effectiveness), according to the below groupings:

- Failed Requirement/Measure not Met – Addressing the recommendation will directly address a system issue and impact the evaluation rating of the system.
- Improvement Considerations – These additional findings are not directly tethered to meeting a requirement or changing the evaluation outcome.

In general, the System Evaluator should list defensible improvement considerations (e.g., mentioned during numerous operator comments during surveys, serious issue, frequent observation) and refrain from adding recommendations based on "one-off" occurrences or isolated operator feedback.

If the TEMP requires M&S, the System Evaluator presents the M&S results within the appropriate measure of the SER with additional M&S results as appendices if needed. M&S results should include a clear and defined modeling and analysis approach to include model validation, a current performance baseline, the predicted impact, and other associated findings.

6.1.3 SER Review and Approval

The System Evaluator adjudicates SET feedback prior to finalizing the SER. The Executive Director, ITA approves the SER after concurrence by the SEB and OTB Managers. When appropriate, the System Evaluator may also create a separate classified SER report with the results of TI testing and provide a reference to this report in the SER. For major programs (non-delegated systems), upon Executive Director, ITA approval, the System Evaluator forwards the SER to the DOT&E. The DOT&E reviews the SER and provides an LOA 30 calendar days after receipt of the SER documenting concurrence/non-concurrence with the SER and an assessment of the overall conduct of the test.

In parallel to SER development, the System Evaluator develops an SCM. This memorandum summarizes the final results of the evaluation and is used as a formal communication by the Executive Director, ITA to stakeholder organizations of SER results. The System Evaluator submits the draft SCM to the Executive Director, ITA in parallel to the submission of the draft SER for review. Upon SER and SCM signature, the System Evaluator transmits the SCM to the

APM Front Office who then routes the memorandum to stakeholder organizational leadership as documented in the template located in the SEB/OTB document library. The SCM should be transmitted to stakeholder organizations within seven calendar days after the SER approval date.

Upon SER signature, the System Evaluator is also responsible for ensuring all recommendations listed in the SER are documented in the Test Event Tracker. The T&E Manager works with the System Evaluator and PMO to track the implementation status of the SER recommendations.

6.1.4 SER Redress Memorandum

When reporting the results of a Follow-on Test and Evaluation (FOT&E), the System Evaluator will typically produce a SER. When system changes lead to a targeted regression test for a specific area (e.g., cyber resilience), as an alternative to a SER update, the System Evaluator may produce a SER Redress memorandum, summarizing the prior results, vendor changes, and verification activity. The SER Redress memorandum will include any changes to the prior Operational Effectiveness, suitability, and/or Resilience ratings as a result of the regression testing.

7.0 ACCEPTANCE TESTING

This section describes the acceptance testing performed by ATSA, to include roles and responsibilities, required coordination, planning, execution, and reporting.

7.1 Acceptance Testing

ATSA performs ATs on TSE in the following instances:

- Prior to ADE-3 or deployment decisions.
- After initial production, field installation, certain maintenance activities, equipment relocation, and when applicable, integration. This ensures consistency of the manufacturing process and a verification of the TSE MCIL, TSE performance, and TSE operability.
- Prior to and in support of major T&E events, per request (e.g., Readiness Testing and CERT at the TSL, QT at the TSIF, and OT at airports) – Section 7.1.3.1 (SAT/ORT) and Section 7.2.2.4 (ISAT).

ATSA performs AT events listed in **Table 7-1** to verify and validate TSE Operational Effectiveness and Suitability.

Table 7-1: Types of ATs

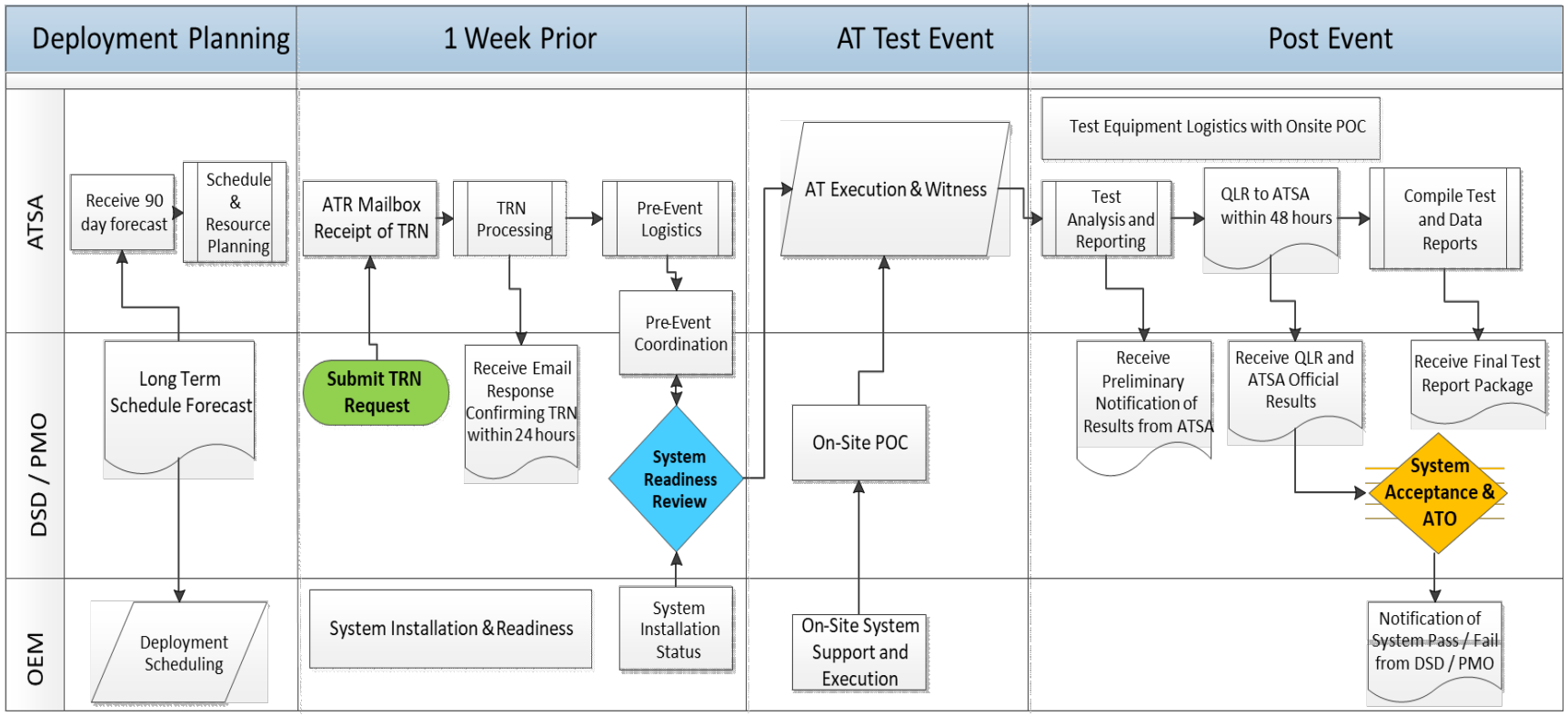
AT Type & Purpose	Supports Decision	Plan & Procedures	Data Collection	Report
First Article Test and Evaluation (FAT&E) FAT&E is a comprehensive test performed at the vendor manufacturing facility on the first TSE unit out of the production line. FAT&E verifies and validates that the first TSE unit meets every requirement listed in the TSE procurement contract RTM.	• TSA production baseline establishment. • Production decision. • Proceed to FAT.	• Author: Vendor • Review & Approval: TSA PMO, ATSA, and DSD	• Testing: Vendor • Observations: TSA PMO, ATSA, and DSD • Duration: up to 2 months • Configuration Audit: DSD/Integrated Logistics Support Full Physical Configuration Audit (PCA) establishes MCIL	• Author: Vendor (QLR) • Observations: TSA PMO and ATSA • Due: 2 weeks after FAT&E
Factory Acceptance Test (FAT) FAT verifies and validates TSA functional capabilities at the vendor facility for every TSE manufactured after the FAT&E per the RTM.	• TSA ownership. • TSA purchase. • TSA deployment.	• Author: Vendor • Review & Approval: ATSA	• Testing: Vendor • Observations: ATSA • Duration: 1 day • Configuration Audit: ATSA validates MCIL	• Author: ATSA (QLR) • Due: 2 weeks after data collection
SAT SAT verifies and validates a subset of TSE operational capabilities deployed to TSA airports prior to operational use per the RTM.	• TSE installation operational decision. • TSA Operations acceptance.	• Author: Vendor • Review & Approval: ATSA	• Testing: ATSA • Assistance: Vendor • Duration: 1 day • Configuration Audit: ATSA validates MCIL	• Author: ATSA • Due: 2 weeks after data collection • QLR

AT Type & Purpose	Supports Decision	Plan & Procedures	Data Collection	Report
ORT ORT is a regression SAT that verifies and validates applicable requirements on TSE after a major repair, corrective maintenance action, upgrades, or relocation.	• See SAT	• See SAT	• See SAT	• See SAT

The AT process is an on-demand process. The TSE vendor works with the relevant PMO to submit an AT TRN for all ATs one (1) week prior to the requested activity to atr@tsa.dhs.gov. For ATs in support of a major T&E event (e.g., CERT, QT, OT), the PMO, or relevant T&E Manager, works with the vendor to submit the AT TRN using the same guidelines. The following sections further describe the AT events in **Table 7-1**. PMOs work with ATSA to plan and budget AT requirements prior to the arrival of the AT TRNs. The AT TRN allows ATSA to allocate resources.

Figure 7-1 illustrates the AT process.

Figure 7-1: AT Process



7.1.1 First Article Test and Evaluation

The First Article Test and Evaluation (FAT&E) ensures that the vendor's first manufactured TSE unit meets all specified requirements. The FAT&E verifies and validates that the TSE will perform as intended in operational environments, thereby supporting TSA's mission needs.

Prior to FAT&E, the PMO and ATSA perform a thorough review of the TSE design specifications, functional requirements, and operational requirements included in the TSE Requirements Traceability Matrix (RTM) in the contract TSA has with the TSE vendor, per the TSAAM and Qualification Policy (see Functional Requirements Matrix). The RTM maps each requirement to one or more verification methods (e.g., testing, inspection, analysis, or demonstration), detailing how and when the vendor will verify each requirement during the FAT&E process. The RTM clarifies the scope of testing, identifies the necessary resources, and delineates the criteria for acceptances or rejection for each requirement to inform the vendor's FAT&E Plan and Procedures. The vendor provides the FAT&E Plan and Procedures to the PMO and the Acceptance Test Director for review and approval.

During FAT&E, the APM CM Specialist performs a full Physical Configuration Audit (PCA) to establish the configuration baseline. That PCA will establish the TSE's MCIL to ensure the TSE are configured correctly prior to all subsequent test events. After the FAT&E, the APM CM Specialist establishes the APM production MCIL (based on the OEM Configuration Items List and ATCB CM Audit report) subsequent to FAT&E, for systems awarded a purchase/deployment contract post ADE-3 decision making. ATSA will perform an MCIL verification during future AT events (e.g., FAT, SAT, or ORT) to verify the TSE has the correct hardware and software listed in the MCIL.

The PMO oversees the vendor conducting FAT&E with ATSA serving as a witness. The vendor must successfully complete FAT&E prior to proceeding with any subsequent TSE production unless the corresponding PMO directs otherwise. FAT&E is integral to the acquisition process, providing assurance of equipment capability and readiness before full-scale production and deployment. FAT&E mitigates risks associated with fielding unproven equipment and ensures that TSA's investments yield effective and reliable solutions for mission-critical operations. The vendor provides the FAT&E Report to the PMO and ATSA for review and approval.

7.1.2 Factory Acceptance Test

The Factory Acceptance Test (FAT) ensures that vendor-manufactured TSE adheres to the specified requirements. The FAT verifies the functionality and performance of the TSE in a controlled factory setting before DSD and the vendor deploy the TSE to designated airports.

Prior to FAT, the vendor develops the FAT Plan and Procedures, outlining the scope, methods, criteria, and schedule of testing based on the RTM, ensuring all contractual requirements are thoroughly tested. The vendor provides the FAT Plan and Procedures to the PMO and the Acceptance Test Director for review and approval.

The vendor conducts the FAT at the manufacturing facility under simulated operational conditions that the TSE will encounter in service. ATSA, along with the PMO and DSD, witness the FAT to ensure compliance with the RTM to ensure proper functionality of the TSE.

ATSA develops the FAT QLR, documenting the test results and compliance status of the TSE (See Section 7.1.4).

The vendor maintains the FAT Plan and Procedures and updates it as TSE changes dictate. The vendor routes any changes to the PMO and Acceptance Test Director for review and approval.

The FAT serves as a critical checkpoint before the TSE enters operational use, ensuring only fully compliant and functional TSE is deployed to the designated airports. This step is vital for ensuring the effectiveness, reliability, and safety of equipment used in TSA operations. Once a TSE passes a FAT, the Government takes ownership of the TSE, and the vendor affixes a TSA barcode on the TSE.

The vendor maintains the FAT Plan and Procedures and updates them as TSE changes packages dictate. PMO and ITA designated Tier 3 changes (Section 3.8) may require AT Plan and Procedure updates, which the vendor must route to PMO and the Acceptance Test Director for review and approval. As part of the change package review process, ATSA and the vendor may perform a FAT dry run on an available TSE at the vendor facility. During this dry run, the vendor will red line the FAT Plan and Procedures for any changes or omissions. If no TSE is available at the vendor facility or TSA facility (e.g., TSL or TSIF), then the vendor will work with the PMO and the Acceptance Test Director to red line the FAT Plan and Procedures during the first FAT after TSA has implemented the change package.

7.1.2.1 Donations: FAT

The Donor-selected testing organization shall perform a FAT on all Donated TSE that are on the Acceptable Capability List (ACL), at the TSE vendor's manufacturing facility or designated location other than the location of final installation. See *Test and Evaluation Division (TED) Support to Third Party Testing for Donated Systems,* dated September 05, 2023, for additional information.

7.1.3 SAT and ORT

The SAT and ORT are essential to validate that TSE perform effectively in its operational environment at the airport. The SAT and ORT are critical for ensuring that the equipment meets operational requirements and is ready for TSA operations.

Prior to the SAT or ORT, the vendor develops the SAT/ORT Plan and Procedures detailing the SAT scope, procedures, criteria, and schedule based on the RTM, ensuring the TSE's operational requirements and specifications are thoroughly tested. The vendor provides the SAT/ORT Plan and Procedures to the PMO and the Acceptance Test Director for review and approval.

SATs are designated for initial TSE installations at an airport; whereas ORTs are essentially regression SATs designated for already installed TSE that undergo major repair, corrective maintenance action, upgrades, or relocation. ORTs may use a subset of the SAT/ORT Plan and Procedures, depending on the Acceptance Test Director's review of the change requiring the ORT.

ATSA performs SATs and ORTs at the airport, where the vendor and DSD install the TSE. ATSA will ask the vendor and/or airport personnel to assist with the SAT/ORT. The SAT/ORT simulates real-world operational conditions to validate the functionality and performance of the TSE's ability to meet all operational requirements per the RTM.

ATSA analyzes the SAT/ORT data against criteria and develops the SAT/ORT QLR documenting any TSE limitations that the vendor may have to address in coordination with the PMO and DSD, as well as the compliance status of the TSE (See Section 7.1.4).

The vendor maintains the SAT/ORT Plan and Procedures and updates them as TSE change packages dictate. PMO and ITA designated Tier 3 changes (Section 3.8) may require AT Plan and Procedures updates, which the vendor must route to PMO and the Acceptance Test Director for review and approval. As part of the change package review process, ATSA and the vendor may perform a SAT or ORT dry run on available TSE at the TSIF, vendor facility, or other PMO-designated facility or laboratory. During this dry run, the vendor will red line the SAT/ORT Plan and Procedures for any changes or omissions. If no TSE is available in any TSA or vendor facility (e.g., TSL or TSIF), then the vendor will work with the Acceptance Test Director to red line the SAT/ORT Plan and Procedures during the first SAT/ORT in an operational environment.

7.1.3.1 SAT / ORT prior to Major T&E Events

The TTB, DGCA, other TSA Laboratory Test Team, and/or OTB, in coordination with the TSA PMO, may choose to have ATSA conduct a SAT or ORT for the TSE prior to a test event at the corresponding laboratory facility or airport. In some instances, the respective Test Team needing a SAT or ORT may coordinate with ATSA to conduct the SAT or ORT themselves (e.g., TSIF Test Team and vendor conducting a SAT at the TSIF). The vendor conducts the SAT with ATSA, or respective Test Team, for newly installed TSE while conducting an ORT for relocated or upgraded TSE that have already had a SAT prior to major T&E Event (e.g., CRT, CERT, QT, OT, etc.). If the respective Test Team requires ATSA to conduct the SAT or ORT prior to the test event, then the Test Team will coordinate with the PMO, T&E Manager, and vendor to submit the AT TRN at least one (1) week prior to the test event. The SAT or ORT ensures the TSE, or TSE update/change, functions as documented in the vendor's QDP or change package documentation. The PMO may work with the vendor to provide ATSA and the Test Team with the current TSE MCIL to verify if different than the MCIL listed in the vendor's SAT/ORT Plan and Procedures.

7.1.3.2 Donations: SAT

The Donor-selected testing organization shall perform the SAT once the TSE vendor installs the TSE in its designed airport. The Donor SAT ensures that the TSE is operational and has the current approved operational software installed.

The Donor ensures that the installed TSE configuration conforms with approved TSA designs, the *Checkpoint Requirements and Planning Guide,* dated May 2020, the ACL, and the CAMB-approved TSE configuration. The ACL provides all acceptable capabilities currently able to be donated to TSA. Capabilities are considered acceptable based on the approval of applicable

ADEs within the ALF. See TED Support to Third Party Testing for Donated Systems for additional information.

7.1.4 AT Reporting

ATSA assigns the TSE one of the following statuses in the AT (e.g., FAT, SAT, or ORT) QLR:

- *TSE Does Not Present any Operational or Safety Concerns (Pass)* – The TSE under test met all criteria specified within the test procedures and, therefore, is ready for operational use.
- *TSE Does Not Present any Operational or Safety Concerns (Deficiencies)* – The TSE under test has anomalies that are outside of the TSE requirements, or other issues of concern that can potentially impact operational use. Anomalies are any condition that deviates from expectations based on program documentation or from someone's perceptions or experiences. Anomalies may be found during, but not limited to, the review, test, analysis, compilation, use, or applicable documentation
- *TSE Presents Either Operational or Safety Concerns (Fail)* –The TSE under test did not meet the TSE requirements or criteria specified within the procedures, or is not ready for operational use.

ATSA provides a 24-hour window where ATSA will remain onsite, if available, that will allow the vendor to diagnose and correct TSE limitations upon notification of an AT Report (e.g., QLR) that specifies a "Fail" status. If the vendor cannot mitigate the TSE limitation in 24-hours, ATSA will depart the site and the vendor and PMO will need to submit a new AT TRN at least one week prior to the requested AT date.

7.1.4.1 Donations: AT Results

CAMB shall coordinate with the PMO to obtain the most current vendor TSE AT Plans and Procedures and coordinate with ATSA to obtain the most current AT QLR Template for the donated TSE.

CAMB shall coordinate with ATSA to obtain the most current Integration Testing procedures (e.g., Network Throughput Test [NTT] or ISAT) and QLR and Test Summary Report (TSR) templates for the donated TSE.

Upon receipt from the Donor-selected Test Team, CAMB will send QLRs to ATSA. ATSA will review the QLR and provide one of the following comments within 48 hours:

- TSE Does Not Present Any Operational or Safety Concerns
- TSE Does Not Present any Operational or Safety Concerns; however, the Donor must correct deficiencies
- TSE Does Not Meet TSA's Functional Requirements Document but Does Not Present any Operational or Security Concerns
- TSE Presents Either Operational or Safety Concerns

CAMB shall determine the Donated TSE's PASS or FAIL status. CAMB coordinates all technical and procedural questions with the appropriate TSA Stakeholders, as needed. CAMB will coordinate with the corresponding APM PMO for all matters dealing with the donation process for all TSE. ATSA will provide CAMB with AT consultation. See TED Support to Third Party Testing for Donated Systems for additional information.

7.2 Integration Acceptance Testing

ATSA performs Integration AT events listed in **Table 7-2** to verify and validate TSE performance.

Table 7-2: Types of Integration ATs

Acceptance Test Type & Purpose	Supports Decision	Plan & Procedures	Data Collection	Report
NTT The NTT validates the functionality of the vendor-installed network in the checkpoint, if applicable, and communication between components upon vendor TSE installation and integration.	• TSE installation operational decision	• Author: Vendor • Review & Approval: ATSA	• Testing: ATSA • Assistance: Vendor • Duration: 1 day	• Author: ATSA • Due: 2 weeks after data collection
ISAT ISAT verifies and validates inline Checked Baggage Inspection System (CBIS) performance, consisting of an integrated Explosives Detection System (EDS) and checked baggage conveyance system (e.g., Baggage Handling System [BHS]) functionality meets or exceeds the site-specific operational requirements.	• TSE installation and BHS integration operational decision	• Author: ATSA	• Testing: ATSA • Assistance: Airport Authority, Local TSA, Vendor	• Author: ATSA (QLR) • Due: 5 days after data collection
Operational Run-In The Operational Run-in will commence two weeks after the completion of the ISAT to assess if BHS and CBIS are performing adequately and within established efficiency requirements.	• TSE installation and BHS integration operational decision	• Author: ATSA	• Testing: Review of BHS and EDS reports from live operations • Assistance: Regional Deployment Coordinator (RDC), BHS Designer and Programmer, EDS Vendor • Duration: 2+ weeks	• Author: ATSA (TSR) • Due: 45 days after data collection

The Integrated AT process is an on-demand process. Prior to commencing Integrated AT, the Project Sponsor must complete the Pre-ISAT TRR and Owner's Testing and documentation. DSD must provide ATSA an AT TRN for all Integrated AT one (1) week prior to the requested activity to atr@tsa.dhs.gov.

For Integrated AT in support of a major T&E event (e.g., OT), the relevant T&E Division Branch/Team submits the Integrated AT TRN using the same guidelines. The following sections further describe the Integrated AT events in Table 7-2.

7.2.1 Network Throughput Test

The Network Throughput Test (NTT) validates the functional capabilities of the networked components of TSE at the airport, ensuring they meet operational requirements for data communication and processing. DSD must provide ATSA an Integrated AT TRN one (1) week prior to the requested activity (see 6.2 above).

The Acceptance Test Director develops the NTT Plan and Procedures detailing the scope, objectives, procedures, and performance criteria. The plan focuses on assessing the network reliability, data throughput, and integration of networked components.

ATSA performs the NTT at the airport upon satisfactory completion of a SAT, ORT, or ISAT if the TSE includes a closed vendor network required for operational performance. The NTT includes assessing then network's ability to handle data traffic, process and record image information efficiently, and maintain stability under veracious loaded conditions. The NTT involves rigorous evaluation of network components, including hardware, software, and data communication protocols. The NTT does not include any cyber security or cyber resilience test methodology (e.g., penetration, protocol examination, network configuration verification, etc.).

If the NTT found the checkpoint TSE network is secure and efficient, ATSA will recommend proceeding to Live Screening Operations. Once a TSE network passes NTT, ATSA in coordination/consultation with the DSD and PMO, will determine the next steps in the process, to include the reporting requirements. If the NTT found the TSE network does not function as intended, preventing TSA for using it in a timely and accurate manner, ATSA will deem the TSE network as a "Fail", and will require another NTT once the vendor, DSD, and PMO addresses and mitigates all deficiencies. ATSA will not perform a retest for at least five (5) business days after the failure and not without a written corrective action report from the vendor, DSD, and or PMO. DSD, PMO, and ATSA will coordinate the timeline for the retest. ATSA treats the retest just like another phase of the NTT.

ATSA analyzes the NTT data against criteria and develops the NTT QLR documenting any TSE network limitations that the vendor may have to address in coordination with the PMO and DSD (Section 7.2.5).

Once a TSE passes an NTT, and assuming the SAT/ORT results are also satisfactory, the airport can use the TSE and Network to screen passengers and/or baggage. Caveat, in some circumstances, IT/IAD may perform testing that corresponding program office, capability manager, and Security Operations may use to determine if the airport can use the TSE and Network to screen passengers and/or baggage.

7.2.1.1 Donations: NTT

The Donor-selected testing organization shall perform the NTT after completing all ISATs for the entire project. The NTT ensures that the network is capable of handling the network traffic expected during full operation of all screening lanes. The Donor shall connect all nodes, TSE, and technologies to the TSE network or infrastructure network at the time of NTT.

The Donor, TSE vendor, or System Integrator shall provide a network diagram with IP Addresses to the Donor-selected testing organization.

The Donor shall plan for the number of NTT days necessary based on the complexity of the Security Operations concept of operations and number of screening lanes. The Donor shall use estimate five (5) business days for the initial NTT estimate. The Donor shall coordinate, fund, implement, and provide the NTT results to CAMB and ATSA.

The Donor, Donor-selected testing organization, TSE vendor, and System Integrator shall collaborate to determine the NTT scope. The Donor and CAMB will provide ATSA with the NTT plan prior to conducting the NTT and the NTT report afterwards for review and comment.

See TED Support to Third Party Testing for Donated Systems for additional information.

7.2.2 Integrated System Acceptance Test

ATSA conducts an ISAT of the Baggage Handling System (BHS) from the ticket counters through the Checked Baggage Resolution Area (CBRA). This includes the tracking, security, safety, reporting and efficiency of the BHS when used in operational scenarios. An ISAT does not include the sortation system or baggage claim areas. ATSA performs ISATs during the phased construction and or at the end of all construction to satisfy the contractual requirement of the DSD Other Transactional Agreement to verify that the BHS procured matches the design specifications and Planning Guidelines and Design Standards (PGDS) requirements.

A BHS provides sortation and conveyance of checked baggage from airport inputs to baggage makeup areas. The CBIS, as part of the BHS, is the portion of the BHS located in the Security Tracking Zone (STZ). The STZ starts at the point at which the BHS acquires positive tracking of a bag prior to the Explosive Detection System (EDS) (normally at a baggage measurement array, an Automatic Tag Reader (ATR), or a photocell where the BHS Tracking Identifier is assigned). The STZ extends to the Clear Line diversion points and to the Baggage Removal Points in the CBRA.

The APM/Checked Baggage Portfolio Planning Branch and DSD require ATSA to perform an ISAT of a CBIS after:

- Construction for a completely new CBIS.
- Each major phase of a multi-phase CBIS project.
- Each construction phase of CBIS with a temporary STZ.

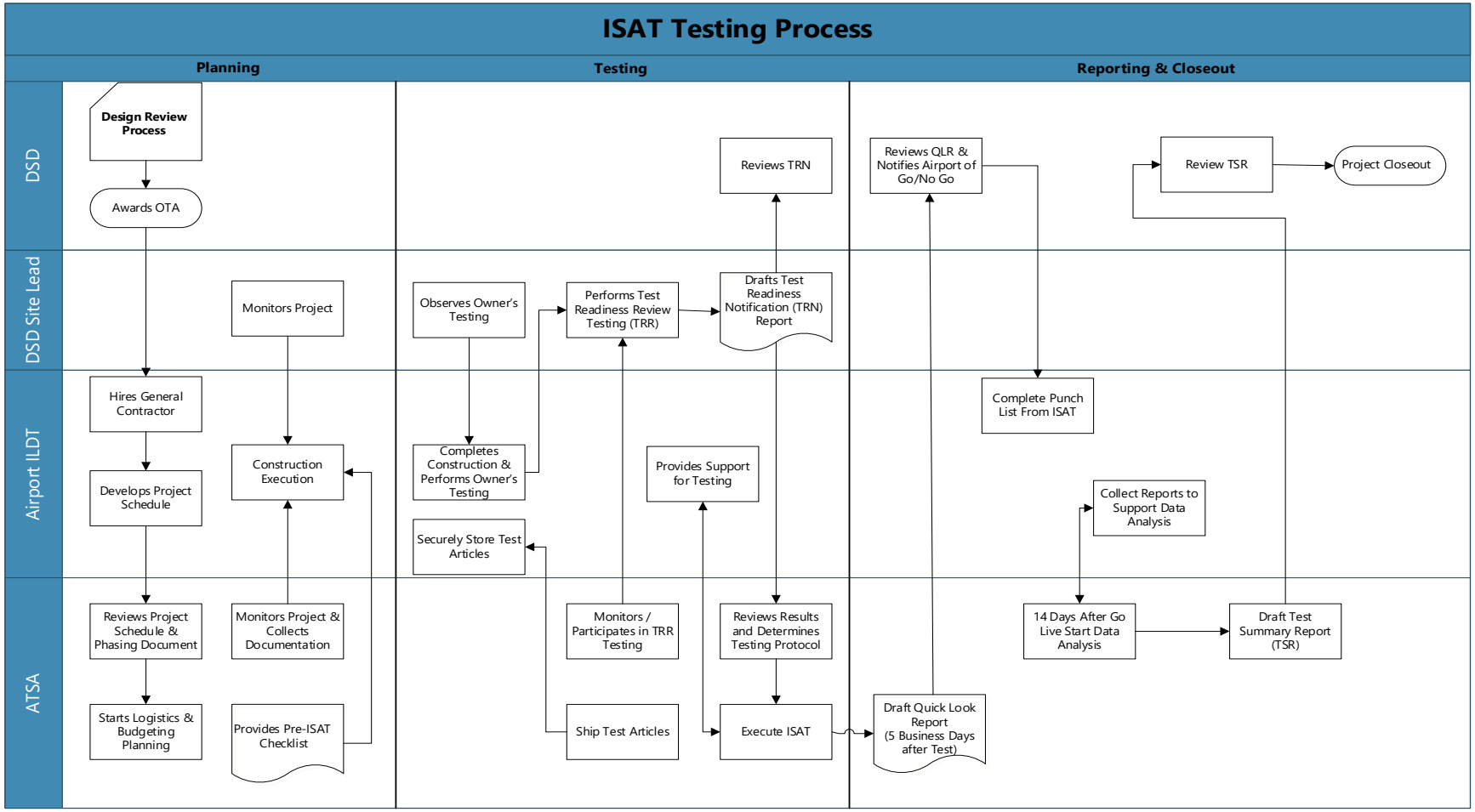
The ISAT process consists of three phases:

1. Pre-ISAT Coordination

2. ISAT Testing
3. ISAT Analysis

Figure 7-2: ISAT Process shows a process flowchart, which provides the tasks and a high-level overview of the ISAT Process through all three phases. There are instances where steps are combined within a phase, but the functions will not transfer between phases.

Figure 7-2: ISAT Process



7.2.2.1 Pre-ISAT (Owner's Testing) Coordination Phase

See PGDS, dated December 30, 2022, section titled *Testing and Commissioning Phase: Testing and Commissioning Phase Overview, Pre-Commissioning Requirements, and Testing and Commissioning Phase Deliverables*

ATSA designed the Pre-ISAT Coordination phase to get involved with the Integrated Local Design Team (ILDT)/Airport Team early in the project to ensure there is a continuous dialog as it relates to the scheduling, conduct, and expectations. At the discretion of the DSD Regional Deployment Coordinator (RDC), the RDC will invite ATSA to attend the normal ILDT/Airport meetings to begin the discussions about ISAT, logistics, and coordination. The RDC will involve ATSA in these early planning meetings, which greatly enhance the successful completion of the overall CBIS project.

ATSA shall provide a Pre-ISAT checklist of required CBIS and logistics information to the ILDT/Airport Team to complete. The ILDT/Airport Team will review this checklist and through a designated POC and provide feedback to the Project Sponsor's Pre-ISAT Team (e.g., Airport Owner or CBIS Operator). ATSA will use this checklist and the subsequent feedback to generate a Project Portfolio that includes, but is not limited to:

- Project Sponsor's testing objective.
- Overall project contact list.
- TSE, BHS, and CBIS descriptions.
- BHS and CBIS drawings.
- TSE serial numbers.
- Expected CBIS throughput.
- Any approved request for variances and/or CBIS CRs.

From the data collected, the Pre-ISAT Team will develop an Owner' Testing strategy and submit it to ATSA for approval. The Pre-ISAT Team will provide the Project Portfolio to ATSA no later than 30 days prior to the ISAT date. For ISATs or Airport projects that require multiple phases, the Pre-ISAT Team shall provide a Project Portfolio and Test Cards for each phase of the project.

The ATSA Pre-ISAT Coordination POC is the primary contact between the ILDT/Airport Team and the ATSA throughout the completion of the project to ensure continuity of communication and a smooth testing transition throughout the project.

Once the Project Portfolio is provided to ATSA, ATSA will assign a Lead for the site who will participate in all meetings with the Pre-ISAT Team to ensure they are fully integrated into the ILDT.

7.2.2.2 Pre-ISAT (Owner's Testing) TRR

See Section PGDS, section titled *Testing and Commissioning Phase – Testing and Commissioning Phase Overview, Pre-Commissioning Requirements*

DSD may request that ATSA participate in the Project Sponsor Owner's Testing Pre-ISAT TRR. DSD will direct ATSA to witness or help facilitate the Pre-ISAT TRR tasks to support the site DSD Site Lead during the Pre-ISAT TRR process. This Owner's Testing precedes ATSA's ISAT and is an opportunity for the ATSA Onsite ISAT Team Lead and/or Deputy Onsite ISAT Team Lead, to gain familiarity with the CBIS under test and also collect test data for ISAT efficiency and security determinations.

Prior to commencing an ISAT, the Project Sponsor must complete the Pre-ISAT TRR and Owner's Testing and documentation. DSD must provide ATSA an AT TRN at least one week prior to the commencement of the ISAT.

7.2.2.3 ISAT Execution

See Section PGDS section titled *Testing and Commissioning Phase: Testing and Commissioning Phase Overview, Pre-Commissioning Requirements, Testing and Commissioning Phase Deliverables, TSA Testing and Commissioning Phase Responsibilities, Integrated System Acceptance Testing, ISAT Pre-Execution, ISAT Execution*

ATSA will perform all ISAT functions to include:

- ISAT bag unpacking/repacking
- ISAT bag induction
- EDS On Screen Resolution operation
- CBRA operation
- ISAT data collection
- BHS matrix operations
- BHS or CBIS observation

ATSA performs the ISAT to qualify the CBIS. The actual execution of the ISAT will normally take place over a one-week period per phase.

- Monday: ATSA travels to the site.
- Tuesday through Thursday: ATSA conducts the ISAT.
- Friday: ATSA departs the site, or used as a backup testing day if necessary.

The duration of the ISAT is dependent on the amount of testing time available each day. If there are at least six (6) hours available each day, then ATSA can complete ISAT in two test days if there are no challenges. A shorter available testing time may extend the overall testing window past the planned duration.

The ATSA ISAT Test Team is comprised of up to eight (8) team members

- Onsite ISAT Team Lead
- Deputy Onsite ISAT Team Lead
- Six (6) ISAT Team Members

ATSA will determine the number of ISAT Team members based on the complexity of the ISAT and the size of the CBIS under test. ATSA's Onsite ISAT Team Lead is the individual responsible for the overall management of the onsite test execution. ATSA will coordinate with all internal and external entities to ensure that the testing is accomplished correctly and in accordance with TSA guidelines. ATSA is the central point of contact for all ISAT activities while onsite. ATSA's Onsite ISAT Team Lead is responsible for the following: ISAT execution, job assignments, ISAT reporting, ISAT data collection, BHS report collection, and TSO training for the test. ATSA's Deputy Onsite ISAT Team Lead is responsible for ensuring that all operations are performed per the test plan and test procedures. In most instances, ATSA will perform any ISAT manipulations or conditions.

ATSA will utilize various ISAT protocols to determine if the CBIS is secure and efficient for TSA Operations. ATSA will perform ISAT based on Appendix D of the PGDS current at the time of testing. Based on the findings of Security and Efficiency, ATSA will provide a recommendation to the RDC as to whether the CBIS has sufficient efficiency and security for live screening operations. The RDC will provide the "Go Live" notification at their discretion.

7.2.2.4 ISAT prior to Operational Testing

The OTB will coordinate with the PMO T&E Manager, DSD, and airport to submit an Integrated AT TRN for an ISAT prior to an OT. ATSA conducts an OT ISAT upon completion of the installation, integration of the TSE under test, and one week after receipt of the Integrated AT TRN. ISATs generally apply to integrated EDS. As opposed to a regular ISAT, an ISAT in support of OT does not require a formal TRR to kick off testing activities.

Upon ISAT completion, ATSA gathers data and reports from the EDS and BHS for data reconciliation, and generates an ISAT QLR within five (5) business days after the completion of the ISAT. ATSA provides the QLR to the System Evaluator and the PMO. ATSA does not provide an ISAT TSR for ISATs in support of an OT.

7.2.2.5 Donations: ISAT

The Donor-selected testing organization shall perform the ISAT once the TSE vendor installs the TSE and the Donor or System Integrator integrates all of the components. The ISAT ensures that all TSE components work together, and all functionality operates per the Security Operations CONOPs document and FRD. CAMB expects the Donor to have the integrated TSE ready to screen passengers before the Donor-selected testing organizations starts the ISAT.

The Donor should plan for approximately two (2) business days per TSE lane. The Donor shall coordinate, fund, implement, and provide the ISAT results to CAMB and ATSA.

See TED Support to Third Party Testing for Donated Systems for additional information.

7.2.3 Operational Run-in & Closeout

See Section PGDS section titled *Testing and Commissioning Phase: Pre-Commissioning Requirements, Integrated Site Acceptance Testing, Operational Run-in & Closeout*

The Operational Run-in will commence two weeks after the completion of the ISAT. The Operational Run-in will normally last for two weeks. The ATSA will forward a data analysis plan to the Owner (e.g., Airport) upon completion of the ISAT, which provides a list of items required for the analysis. During the run-in period, ATSA expects that the Owner and the BHS and EDS teams will provide the requested reports to support the data analysis effort. If data shows the CBIS is performing adequately and within established efficiency requirements, the run-in will stop and ATSA will draft the TSR. If performance is not within the established efficiency requirements, or at the discretion of the RDC, the Owner will perform another two weeks of data collection and run-in prior ATSA drafting the TSR.

Upon completion of the two week (or as prescribed) run-in period, ATSA will perform an analysis of the Owner's submitted reports. ATSA will draft and issue the TSR to the RDC. The RDC will then provide the TSR to the ILDT/Airport Team.

ATSA requires the Owner's Data Analysis Plan, BHS reports, and EDS reports.

ATSA will provide the ISAT results and the TSR.

In order to have a successful ISAT, the Owner's TRR and testing should ensure that the CBIS performs in accordance with the PGDS requirements. If the Owner's testing, as outlined in PGDS Appendix D, is successfully completed, then the CBIS should pass the ISAT.

7.2.4 ISAT and Operational Run-in Data Analysis

See Section PGDS section titled *Testing and Commissioning Phase: Pre-Commissioning Requirements, Testing and Commissioning Phase Deliverables, Operational Run-in & Closeout*

ATSA's Data Analysis Team delivers an ISAT Analysis Plan to the ILDT/Airport Team at least 14 calendar days prior to the requested data collection. This plan is a step-by-step guide on what reports ATSA needs from the airport to accurately assess the operation of the CBIS. Additionally, this plan outlines how the Project Sponsor (e.g., Airport Owner or CBIS Operator) should provide ATSA the BHS reports.

ATSA's Data Analysis Team is responsible for all data analysis of the test data for all phases of the project. During the ISAT test execution, ATSA's Onsite ISAT Team Lead or Deputy Onsite ISAT Team Lead will forward the test data collected during the tests on a daily basis to ATSA's Data Analysis Team for analysis. The Data Analysis Team provides analysis of the test data for the ISAT QLR (after ISAT) or ISAT TSR (after ISAT and Operational Run-in) to the Onsite ISAT Team Lead in a timely manner to allow the delivery of the reports within five (5) business days upon completion of ISAT or Operational Run-in. The Operational Run-in will commence two weeks after the completion of the ISAT unless ATSA designates otherwise. The Operational Run-in will normally last for two weeks but may extend if conditions warrant it.

During the Operational Run-in period, ATSA expects that the Project Sponsor and the BHS and EDS Teams will provide the requested reports to support the data analysis effort. If ATSA determines that the CBIS is performing adequately and within established efficiency requirements, the run-in will stop and ATSA will draft the QLR or TSR. If performance is not within the established efficiency requirements, or at the discretion of the RDC, the Owner will perform another two weeks of data collection and Operational Run-in prior to ATSA drafting the QLR or TSR.

Upon completion of the two (2) week (or as prescribed) Operational Run-in period, ATSA will perform an analysis of the Owner's submitted reports. ATSA will analyze the data for incorporation into the ISAT QLR or TSR.

The ISAT TSR will include the results from all testing (Owner's TRR and ATSA's ISAT) as well as data from the Operational Run-in. Additionally, it will include a running list of all items discovered and the status of those items. The ISAT TSR should also detail any new findings.

ATSA will finalize, approve, and forward the ISAT TSR to the RDC and the any other key stakeholders (e.g., DSD Site Lead, T&E Division, Checked Baggage Planning Branch). The RDC will then provide the ISAT TSR to the ILDT/Airport Team.

7.2.5 Integration Testing Reporting

See Section PGDS section titled *Testing and Commissioning Phase: Pre-Commissioning Requirements, Testing and Commissioning Phase Deliverables, ISAT Execution, Operational Run-in & Closeout*

The ATSA Lead is responsible for drafting the ISAT QLR and TSR. The Integrated Acceptance Test Director reviews and approves the QLR and TSR for distribution. ATSA will deliver an ISAT QLR after each airport project or project phase. ATSA only provides a TSR after the final phase of the project when local TSA starts live screening operations. The TSR is a summary of all outstanding items and a synopsis of all testing to date.

ATSA submits the ISAT QLR reports within five (5) business days after completion of ISAT, or in the case of TSRs, within five (5) business days after collection of data during the Operational Run-in period (Section 7.2.3).

The QLR is a formal synopsis of the ISAT results and provides a recommendation to DSD as to the status if the CBIS.

ATSA will deliver a TSR as the final testing report (to include Operational Run-in) for a CBIS project within 45 days after the airport started screening checked luggage using the CBIS. The TSR outlines the status of CBIS deficiencies and provides Efficiency and Suitability determinations based on actual live operations.

The QLR and TSR shall provide recommendations on the following:

- Whether the CBIS should proceed to live screening operations
- Whether the CBIS has adequate *security* for live screening operations
- Whether the CBIS has sufficient *efficiency* for live screening operations

These recommendations are based on the information collected during the testing of the CBIS. ATSA determines CBIS security based on the CBIS properly tracking and sorting clear bags to makeup and alarmed bags to CBRA correctly. ATSA determines CBIS efficiency based on how well the CBIS operates in relation to the efficiency standards outlined in the PGDS and Basis of Design documentation.

If the ISAT found the CBIS is "secure" and "efficient" (i.e., no safety, security, or efficiency challenges), ATSA will recommend proceeding to Live Screening Operations. Once a CBIS passes ISAT, ATSA in coordination/consultation with the RDC, will determine the next steps in the process, to include the reporting requirements for multi-phased projects. If the ISAT found the CBIS is not "secure", due to safety or security challenges that negatively impact operations or personnel, ATSA will deem the CBIS as a "Fail", and will require another ISAT once the Owner addresses and corrects all deficiencies. ATSA will not perform a retest for at least five (5) business days after the failure. ATSA will not perform a retest without a written corrective action report from the Airport Owner (e.g., Airport Project Sponsor, CBIS Operator) and a new AT TRN. The RDC and ATSA will coordinate the timeline for the retest. ATSA treats the retest just like another phase of the ISAT. If a CBIS fails ISAT, then the BHS developer would need to make a major BHS programming change to correct the deficiencies.

7.2.5.1 Donations: Integration Test Results

CAMB shall coordinate with the PMO to obtain the most current AT Plans and Procedures for the donated TSE. CAMB shall coordinate with ATSA to obtain the most current Integration Testing procedures (e.g., NTT or ISAT) and QLR and TSR templates.

CAMB will send QLRs to ATSA. ATSA will review the QLR and provide one of the following comments within 48 hours:

- TSE Does Not Present Any Operational or Safety Concerns
- TSE Does Not Present any Operational or Safety Concerns; however, the Donor must correct deficiencies
- TSE Does Not Meet TSA's Functional Requirements Document but Does Not Present any Operational or Security Concerns
- TSE Presents Either Operational or Safety Concerns

CAMB shall determine the Donation's PASS or FAIL status. CAMB coordinate all technical and procedural questions with the appropriate TSA Stakeholders, as needed. CAMB will coordinate with the corresponding APM PMO for all matters dealing with the donation process for all TSE. ATSA will provide CAMB with AT consultation.

7.3 Baggage Assessment and System Evaluation

The Baggage Assessment and Systems Evaluation (BASE) Team, an independent group within the TSA's T&E Division/ATSA, plays a pivotal role in enhancing airport checked baggage security and efficiency. The BASE Team determines the operational integrity of the CBIS and BHS. With a focus on the CBIS, the BASE Team collaborates with TSA operations, airports, and airlines to identify and rectify vulnerabilities in these critical infrastructures to maximize the

Operational Effectiveness and develop actionable solutions, ensuring CBIS operates at peak performance.

7.3.1 CBIS PGDS

The ATSA BASE Team authors the PGDS for CBIS. The purpose of the PGDS is to present TSA's requirements and documented best practices for implementing a high-performance and cost-effective CBIS. The PGDS captures TSA's requirements for a CBIS project from the beginning stages of design through commissioning of the system. Best practices are meant to highlight practices that have proven successful during implementation and that TSA recommends for the Project Sponsor's (e.g., Airport Owner or CBIS Operator) consideration during the design and construction of a CBIS.

7.3.2 BHS CBIS Support

The ATSA BASE Team plays a vital role in supporting TSA airports' BHS and CBIS.

A BHS provides sortation and conveyance of checked baggage from airport inputs to baggage makeup areas.

The CBIS, as part of the BHS, is the portion of the BHS located in the STZ. The STZ starts at the point at which the BHS acquires positive tracking of a bag prior to the EDS (normally at a baggage measurement array, an ATR, or a photocell where the BHS Tracking Identifier is assigned). The STZ extends to the Clear Line diversion points and to the Baggage Removal Points in the CBRA.

The BASE Team coordinates with airport stakeholders, ensuring BHS and CBIS integrity, and troubleshooting operational issues. The BASE Team's expertise in BHS and CBIS is crucial for maintaining optimal performance and addressing challenges that may arise in real-time operational environments.

7.3.3 CBIS Design Reviews

The ATSA BASE Team conducts detailed CBIS Design Reviews, PGDS Requests for Variance(RSV) reviews, and CBIS CR reviews. These reviews involve an assessment of design proposals, ensuring compliance with the latest PGDS, TSA standards, and providing SME recommendations.

BASE Team CBIS Design Reviews are integral to the successful implementation of CBIS, ensuring Project Sponsors (e.g., Airport Owner or CBIS Operator) design CBIS for optimal functionality and security.

- CBIS Design Reviews: See PGDS Design Review Process
- CBIS CRs: See PGDS CBIS CR
- PGDS RSV: See PGDS RSV

7.3.4 BASE Efforts

ATSA BASE Team efforts extend beyond design and support to encompass a wide range of activities, including CBIS evaluations, CBIS process optimizations, and continuous CBIS improvement initiatives. The BASE Team efforts are essential in enhancing the efficiency and effectiveness of CBIS.

- BHS and CBIS Support: The BASE Team supports TSA's airports by ensuring the smooth operation of BHS and CBIS, focusing on the STZ where the precise tracking and screening of baggage occur. This includes troubleshooting operational issues and maintaining system integrity.
- CBIS PGDS: As authors of the PGDS, the BASE Team sets forth TSA's requirements and best practices for designing and implementing efficient, cost-effective CBIS. These guidelines serve as a blueprint from the initial design stages through the commissioning of the system, incorporating successful practices recommended for project sponsors.
- CBIS Design Reviews: Conducting thorough design, change request, and RSV reviews, the BASE Team ensures compliance with TSA standards and PGDS. These reviews are crucial for the successful implementation of CBIS, guiding project sponsors towards optimal functionality and security.
- R&D: Engaging in R&D, the BASE Team explores innovative solutions and technologies to advance CBIS capabilities. Through studies, pilot projects, and industry collaborations, the team integrates cutting-edge solutions into TSA's operational framework.
- Laboratory/Facility BHS Support: The BASE Team provides essential support to the BHS at both the TSIF and the TSA Logistics Center (TSALC) BHS Loop. This support includes evaluating performance, ensuring PGDS compliance, and conducting ISATs and regression testing for BHS enhancements.

Enhancing the efficiency and security of CBIS and BHS is critical for safeguarding the nation's transportation systems. By identifying vulnerabilities, implementing best practices, and incorporating innovative technologies, the BASE Team ensures TSA's readiness to meet and mitigate threats.

Through a collaborative approach, the BASE Team brings together TSA operations, airports, airlines, and technology providers. By focusing on common goals, the team facilitates improvements that enhance the overall security and efficiency of baggage inspection and handling processes.

7.3.5 CBIS R&D

The ATSA BASE Team researches and develops innovative solutions and technologies (e.g., dimensioning and automated bag tracking technologies) for CBIS. The BASE Team engages in studies, pilot projects, and collaborations industry partners to advance the field and integrate cutting-edge solutions into TSA's operational framework.

7.4 Laboratory/Facility BHS Support

7.4.1 TSIF BHS

ATSA provides essential support to the BHS at the TSIF. This support includes evaluating the TSIF BHS performance, efficiency, and compatibility with various EDS. The TSIF BHS has five lanes for EDS under TSA Acquisition and one additional lane for developmental EDS. ATSA's involvement at the TSIF ensure that the BHS operates seamlessly with new EDS integrations, is PGDS-compliant, and facilitates realistic simulations and tests that mirror airport operations. This support is critical for validating the Effectiveness of EDS equipment that TSA expects to integrate with various BHS providers across the country before DSD deploys them. ATSA also performs ISATs for the TSIF BHS, and any regression testing needed on BHS enhancements.

7.4.2 TSALC BHS Loop

ATSA mains and operates the BHS Loop at the TSALC, where ATSA is based. This involvement includes overseeing the operational testing BHS equipment within a controlled BHS environment. ATSA's CBIS expertise ensures that the BHS loop is consistently updated and maintained to reflect current operational standards and challenges. This support enables comprehensive testing and evaluation of screening technologies, aiding in the development of effective and efficient baggage screening solutions that TSA and airports can implement across various airport environments.

7.5 Acceptance Testing and System Assessment Test Articles

ATSA requires Acceptance Test Articles to support a wide range of AT activities across the various security technology platforms. These test articles include image quality phantoms and SOC representative test luggage, and ISAT Articles. The following sections provide descriptions of two types of test articles and their intended purpose.

7.5.1 Image Quality Test Kits

TSE-specific image quality phantoms ensure the proper setup and operation of image-producing security technologies. These specialty phantoms are designed to characterize the imaging subsystem of candidate platforms and provide a quantitative assessment of image quality. These test articles focus on a measurement of specific image quality parameters critical to the operation of the TSE. For further information regarding these image quality phantom kits, please reference:

- The American Society for Testing and Materials (ASTM) F792-08 (or most recent), Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems
- The American National Standards Institute (ANSI) 42.45-2021 (or most recent), American National Standard for Evaluating the Image Quality of X-Ray Computed Tomography Security-Screening Systems. See ATSA's ANSI N42.45 Implementation Plan and Pass/Fail Methodology.

7.5.2 SOC Representative Test Articles

SOC representative test articles are used to evaluate TSE performance during SAT or ORT events. ATSA stores these articles in a central warehouse, maintains a current inventory, and is responsible for shipment of articles to and from the test site.

7.5.3 ISAT Test Articles

ISAT test articles are items that represent the average size outlined in the PGDS. These items do not have normal luggage clutter in them as they have a weighted material in them to allow for normal conveyance and a number identification plate that is used for baggage reconciliation. These items come in a transportable kit that contains between 40 and 50 test articles.

7.5.4 Donations: ATSA Logistical Support

Acceptance Test Articles in support of Donations: The Donor-selected testing organization or Site Integrator shall submit a Test Article request to ATSA via the ATR Inbox (atr@tsa.dhs.gov) with a copy to CAMB. The email shall provide all logistic information about the delivery (location, time, special requirements, and any other notes that will assist in the delivery of the test articles). Upon receipt, ATSA will reach out to the Donor POC to coordinate the shipment of the test articles.

ATSA will provide the test articles necessary for AT. The Donor is responsible for the following costs:

- Cost of shipping of bags to and from test location.
- Coordinating and storing the bags in a secured location that is protected from the elements as much as feasibly possible (if applicable).
- Cost of any damage to test articles due to storage, transportation, or any abusive use (paid to current ATSS contract awardee).

The Donor selected test organization shall maintain and return the test articles to ATSA in the same condition, excluding normal use, as when received after each AT event unless ATSA authorizes a longer period. ATSA will inspect the test articles upon return and assess any damages.

APPENDIX A: ACRONYM LIST

AA	Adversarial Assessment
ACL	Acceptable Capability List
ADA	Acquisition Decision Authority
ADE	Acquisition Decision Event
ADM	Acquisition Decision Memorandum
AI	Additional Issue
ALF	Acquisition Life Cycle Framework
ANSI	American National Standards Institute
APM	Acquisition Program Management
ARB	Acquisition Review Board
ASTM	American Society for Testing Materials
AT	Acceptance Test
ATCB	As-Tested Configuration Baseline
ATR	Automatic Tag Reader
ATSA	Acceptance Test and System Assessment
BASE	Baggage Assessment and Systems Evaluation
BHS	Baggage Handling System
C&P	Contracting and Procurement
CAE	Component Acquisition Executive
CAMB	Capability Acceptance Management Branch
CBIS	Checked Baggage Inspection System
CBRA	Checked Baggage Resolution Area
CCB	Configuration Control Board
CERT	Certification Testing
CI	Configuration Item
CM	Configuration Management
CMD	Capabilities Management Division
CMP	Configuration Management Plan
COI	Critical Operational Issue
COIC	Critical Operational Issues and Criteria

CONOPs	Concept of Operations
CR	Change Request
CVPA	Cooperative Vulnerability and Penetration Assessment
DAG	Data Authentication Group
DCAR	Data Collection Activity Report
DGCA	Designated Government Certification Agent
DHS	Department of Homeland Security
DOT&E	Director, Office of Test and Evaluation
DSD	Deployment and Sustainment Division
DT	Developmental Testing
DTS	Determination of Test Scope
EDS	Explosives Detection System
EF	Evaluation Framework
ERB	Emerging Results Briefing
ESR	Early Strategy Review
FAT	Factory Acceptance Test
FAT&E	First Article Test and Evaluation
FOC	Full Operational Capability
FOT&E	Follow-on Operational Test and Evaluation
FOTP	Follow-on Operational Test Plan
FRD	Functional Requirements Document
FRS	Final Results Summary
FSD	Federal Security Director
GRC	Governance, Risk, and Compliance
IAD	Information Assurance and Cybersecurity Division
ID	Insufficient Data
ILDT	Integrated Local Design Team
IMS	Integrated Master Schedule
IOT&E	Initial Operational Test and Evaluation
IPM	Integrated Process Manual
IPT	Integrated Product Team

ISAT	Integrated Site Acceptance Test
IT	Information Technology
IT&E	Independent Test and Evaluation
ITA	Independent Test Agent
ITF	Innovation Task Force
KPP	Key Performance Parameter
LEO	Law Enforcement Officer
LOA	Letter of Assessment
M&S	Modeling and Simulation
MAOL	Master Acquisition Oversight List
MCIL	Master Configuration Items List
MD	Management Directive
MNS	Mission Needs Statement
NA	Not Applicable
NT	Not Tested
NTT	Network Throughput Test
OA	Operational Assessment
ORD	Operational Requirements Document
ORT	Operational Readiness Test
OSHE	Occupational Safety, Health, and Environment
OT	Operational Test
OTB	Operational Test Branch
OTD	Operational Test Director
OTP	Operational Test Plan
OTRR	Operational Test Readiness Review
OUE	Operational Utility Evaluation
PCA	Physical Configuration Audit
PEO	Program Execution Office
PGDS	Planning Guidelines and Design Standards
PI	Prohibited Item
PM	Program Manager

PMO	Program Management Office
POC	Point of Contact
QDP	Qualification Data Package
QLR	Quick Look Report
QPL	Qualified Products List
QT	Qualification Test
QTD	Qualification Test Director
QTP	Qualification Test Plan
QTR	Qualification Test Report
QTRR	Qualification Test Readiness Review
QVP	Qualification Verification Package
R&D	Research and Development
RCA	Requirements and Capabilities Analysis
RCM	Requirements Crosswalk Matrix
RDC	Regional Deployment Coordinator
RFD	Request for Deviation
RMA	Reliability, Maintainability, and Availability
RQT	Regression Qualification Test
RTM	Requirements Traceability Matrix
SAT	Site Acceptance Test
SCM	System Evaluation Report Communication Memorandum
SEB	System Evaluation Branch
SEP	System Evaluation Plan
SER	System Evaluation Report
SET	System Evaluation Team
SME	Subject Matter Expert
SOC	Stream-of-Commerce
SOP	Standard Operating Procedures
SRR	System Readiness Review
SSA	Site Selection Authority
SSI	Sensitive Security Information

STN	Start of Testing Notification
STZ	Security Tracking Zone
SUT	System Under Test
T&E	Test and Evaluation
TECB	Test and Evaluation Concept Briefing
TEDAC	Terrorist Explosive Device Analytical Center
TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
TI	Threat Inject
TI&O	Test Infrastructure and Operations
TIC	Threat Inject Carrier
TIEDS	Terrorist Explosive Device Analytical Center Improvised Explosives Detection and Synthesis
TIM	Technical Interchange Meeting
TIOB	Test Infrastructure and Operations Branch
TIR	Test Incident Report
TRN	Test Readiness Notification
TRR	Test Readiness Review
TSA	Transportation Security Administration
TSAAM	TSA Acquisition Manual
TSALC	TSA Logistics Center
TSE	Transportation Security Equipment
TSIF	TSA Systems Integration Facility
TSL	Transportation Security Laboratory
TSO	Transportation Security Officer
TSR	Test Summary Report
TTB	TSIF Test Branch
VV&A	Verification, Validation, and Accreditation

APPENDIX B: TEST AND EVALUATION PLANS, REPORTS, AND OTHER SUPPORTING DOCUMENTATION

System Evaluation Branch, Operational Test Branch, and Transportation Security Administration (TSA) Systems Integration Facility Test Branch plans, reports, and document templates are located in the TSA iShare repository. Please contact the TSA test organization manager to request access to these libraries.

APPENDIX C: REFERENCES

Department of Homeland Security

- Acquisition Management Directive 102-01, Revision 3.1, February 25, 2019
- Acquisition Management Instruction 102-01-001, Revision 02, January 10, 2023
- DHS Directive 026-06, Test and Evaluation, Revision 02, October 01, 2020
- DHS Instruction 026-06-001, Test and Evaluation, Revision 1, October 01, 2020
- DHS Supplemental Guidance, Threat Assessment in Support of T&E, Version 1.0, September 2018
- DHS Supplemental Guidance, Cyber Resilience T&E, Version 2.0, October 2019
- DHS Supplemental Guidance, T&E Management, Version 3.0, January 2019
- DHS Instruction Guide 026-06-001-01, Revision 1, Test and Evaluation Master Plan (TEMP), October 3, 2018
- DHS Technical Review Guide, Version 3.0, February 2022
- DOT&E T&E Strategy Brief Memorandum, September 08, 2021
- Reliability, Availability, Maintainability, Test and Evaluation Supplemental Guidance, Version 2.0, September 2022
- Scientific Test and Analysis Techniques, Version 1.0, September 2021

Transportation Security Administration

- Test and Evaluation Management Directive 2600.4, August 21, 2024
- TSIF Events Management, Management Directive 2600.3, April 27, 2022
- TSA Acquisition Qualification Policy, Office of Acquisition Program Management, Version 1.0, December 14, 2017
- TSA Acquisition Manual (TSAAM), Version 3.0, June 2023
- TSA Test and Evaluation Statistical Methodology Policy, April 28, 2016
- TSA Transportation Security Equipment Certification Policy, Version 1.0, April 21, 2021
- TSA Third Party Testing Framework, Version 1.0, October 04, 2021
- TSA Managing Changes to Deployed TSA Systems (APM-19-005), February, 12, 2019
- Data Collection and Analysis Handbook, Revision 1.1, August 27, 2024

- Test and Evaluation Division (TED) Support to Third Party Testing (TPT) for Donated Systems, Version 1.2, September 05, 2023
- Office of Security Capabilities Test and Evaluation Verification, Validation and Accreditation (VV&A) Policy, Version 1.0, May 27, 2014
- Configuration Management Plan (CMP) for Office of Acquisition Program Management, Version E, August 31, 2018
- TSA Systems Integration Facility (TSIF) Test and Test Infrastructure and Operations Integrated Process Manual, Version 6.0, September 6, 2019
- TSA Systems Integration Facility (TSIF) Test Branch and Test Infrastructure and Operations (TI&O) Branch Quality Manual, Version 9.1, August 31, 2022
- TSA Systems Integration Facility (TSIF) Test Branch, Transportation Security Equipment (TSE) Configuration Management Plan (CMP), Version 2.3, June 27, 2022
- Planning Guidelines and Design Standards for Checked Baggage Inspection Systems, Version 8.0, December 30, 2022
- TSA Checkpoint Requirements Planning Guide, May 2020

APPENDIX D: CYBERSECURITY EVALUATION GUIDANCE

The objective of Cybersecurity Test and Evaluation (T&E) activities is to determine whether the system's Operational Cyber Resilience criteria and/or Critical Operational Issue (COI) is met. The Cyber Resilience COI/criteria is a critical component of a systems overall Resilience. The system being tested comprises the hardware, software, operators, maintainers, and the training and Standard Operating Procedures (SOPs) used to carry out the Concept of Operations (CONOPs). The Cyber Resilience evaluation includes test activities to gather sufficient data to identify all significant vulnerabilities of the System Under Test (SUT). The Independent Test Agent (ITA) conducts Cybersecurity T&E in alignment with *DHS Supplemental Guidance, Cyber Resilience T&E,* dated October 2019.

D.1 Ensuring Adequate Cybersecurity T&E

Adequate Cybersecurity T&E requires the selection of an independent entity, separate from an organization's internal Information Technology (IT) department, to plan, execute, and report required cybersecurity test activities. The TSA ITA has extensive cybersecurity T&E capabilities to include the planning, execution, and reporting of Adversarial Assessments (AAs) across a wide range of Information Technology (IT) and non-IT systems.

Adequate cybersecurity T&E requires a commitment by all parties to provide sufficient funding, staffing/resources, and time. The T&E Manager works with the Program Management Office (PMO) when establishing the Integrated Master Schedule (IMS) to ensure the necessary cybersecurity T&E activities are documented across the acquisition life cycle as distinct events. Further, the T&E Manager works with the PMO, ITA, and relevant contract technical monitors to ensure adequate resources are allocated for these activities.

Cybersecurity T&E also requires regular communications across stakeholders via the T&E Working-level Integrated Product Team (WIPT) and the System Evaluation Team (SET) and a common understanding by all parties of cybersecurity T&E roles and responsibilities, particularly between the ITA and the TSA/IT/Information Assurance and Cybersecurity Division (IAD). These roles are expanded upon below:

- ITA – Overall responsibility for the independent evaluation of Resilience and the Cyber Resilience criteria. As authorized by the Department of Homeland Security (DHS) Director, Office of Test and Evaluation (DOT&E), defines cybersecurity T&E strategy, evaluation concept, develops the AA Plan within the Operational Test Plan (OTP), executes the AA, assesses the criticality of vulnerabilities discovered across all cybersecurity T&E activities, and determines the final Resilience rating for a System Under Test (SUT).

- IT/IAD – The internal IT organization responsible for protecting information systems against unauthorized access, use, disclosure, disruption, unauthorized modification, or destruction. In this capacity, IT/IAD ensures systems have the necessary hardening to support deployment and the necessary compliance for connecting to the TSA network (e.g., Authority to Operate [ATO]). IT/IAD conducts CVPAs and Penetration Tests to support these objectives. The ITA can leverage these test results as needed in its overarching Cybersecurity T&E Strategy. The TTB may support IAD with CVPA planning, execution, and reporting for SUTs as necessary.

D.2 Cybersecurity T&E Events

The primary T&E event leveraged by the ITA to assess cyber resilience is the AA. The ITA System Evaluator may also consider additional inputs from the IT IAD-led CVPA, Penetration Testing and other ATO-required security controls assessments as needed.

D.2.1 Cooperative Vulnerability and Penetration Assessment

The CVPA is a DT activity that focuses on hardening the attack surface through the discovery of hardware and software vulnerabilities. The team inspects and analyzes the SUT for cyber-vulnerabilities by running vulnerability scans using appropriate IT Security tools (e.g., Tenable Nessus) combined with a corresponding penetration assessment. The acquisition strategy may allow the correction of CVPA vulnerabilities prior to the AA, or allow those vulnerabilities to remain to assess their impact during the AA. An emphasis on the former (early correction) will help overall cyber resilience outcomes. CVPAs are IT Policy driven and inform organizational IT security decisions. A CVPA is not equal to a Penetration Test, and should never be used in lieu of the DOT&E-required AA.

When scoring CVPA scan results, the vulnerability scanning software typically applies the Common Vulnerability Scoring System (CVSS) to the vulnerability, generating a severity rating using an internal industry standard algorithm. The CVSS vulnerabilities scoring is aligned with the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) and Common Vulnerability and Exposure (CVE) System. As such, scoring conferences are not required for vulnerabilities resulting from scanning software. Vulnerability scoring in these cases should focus less on criticality scoring and more on the applicability of the vulnerability based on the system configuration TSA is looking to deploy. Scoring conferences should be convened for CVPA penetration assessment vulnerabilities to assess their impact to the cyber resilience of the system.

During the CVPA, the test team may also assess the SUT for cybersecurity specific ORD and FRD requirements. As designated in the Evaluation Framework, this activity may instead occur as part of a larger, planned Qualification Test (QT) event, rather than a dedicated CVPA.

D.2.2 AA and Penetration Testing

DHS DOT&E requires an AA as the primary input to the Cyber Resilience determination. An AA assesses the ability of the system to withstand offensive cybersecurity attacks based on the mission threat. To be operationally resilient, the system must remain effective and suitable to satisfy the mission while under duress from offensive cybersecurity attack. A Penetration Test

also assesses the ability to withstand cybersecurity attacks, however, differs from an AA in several key areas as described in **Table D-1**.

Table D-1: AA and Penetration Test Differences

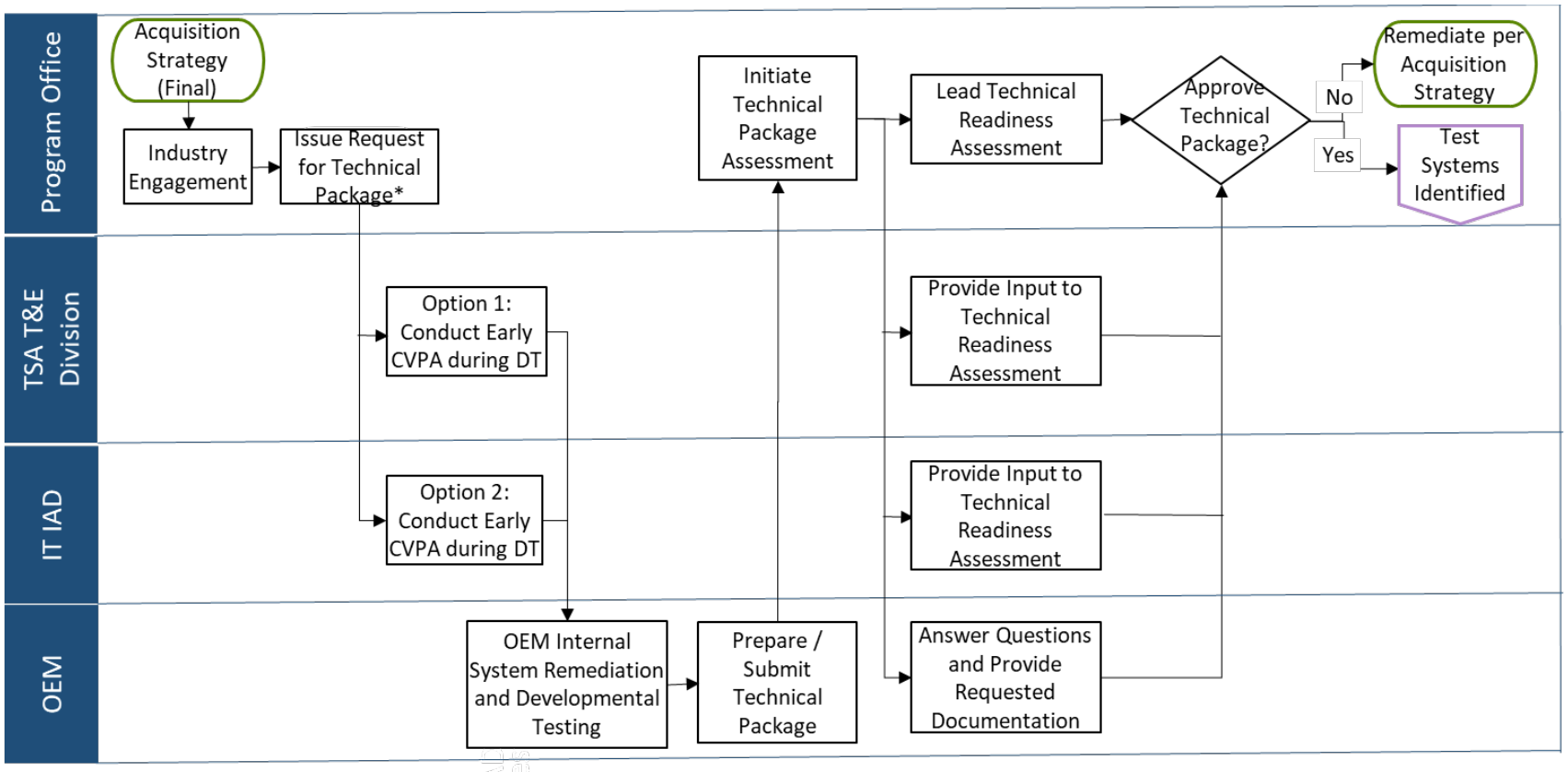
	Adversarial Assessment	Penetration Test
Lead Organization	ITA (TSA T&E Division)	Penetration Test Team (IT IAD)
Use of Results	Inform the ITAs operational resilience rating in the System Evaluation Report	Inform organizational IT security decisions (e.g., authority to operate)
Approver of Results	ITA as part of SER (concurrence from TSA IT desired)	TSA IT IAD
Policy / Guidance	TEMP Driven (DHS DOT&E Approved)	IT Policy Driven (TSA IT Approved)
Timing / Frequency	Performed in support of an ADE-3 for an acquisition program as directed in the TEMP	Recurring basis for deployed connected systems as required by IT Policy
Type	Operational Test / Environment	Developmental Test / Laboratory Environment
Scope	Find and score vulnerabilities considering mission impact (e.g., operate equipment by running bags / phantom / mock passengers to see outcome)	Find vulnerabilities independent of mission effects
	Assess system against User-defined scenarios based on threat assessment and cyber table top exercises	Assess system against standard Enterprise IT defined scenarios

Per the DHS Cyber Resilience T&E Guide page 33: "Penetration Testing Does Not Equal Adversarial Testing."

D.3 Cybersecurity Test and Evaluation Early Engagement with Industry

As part of the PMO-defined Qualification Process, the ITA should encourage early cybersecurity T&E in the form of one or more CVPAs as part of the vendor's DT. This potential engagement is illustrated in **Figure D-1**. The Qualification Process is tailorable across programs.

Figure D-1: Cybersecurity T&E During Early Engagement with Industry



*The exact activities and conditions associated with the Technical Package request, review, and approval will vary from program to program based on its Acquisition Strategy / Qualification Process.

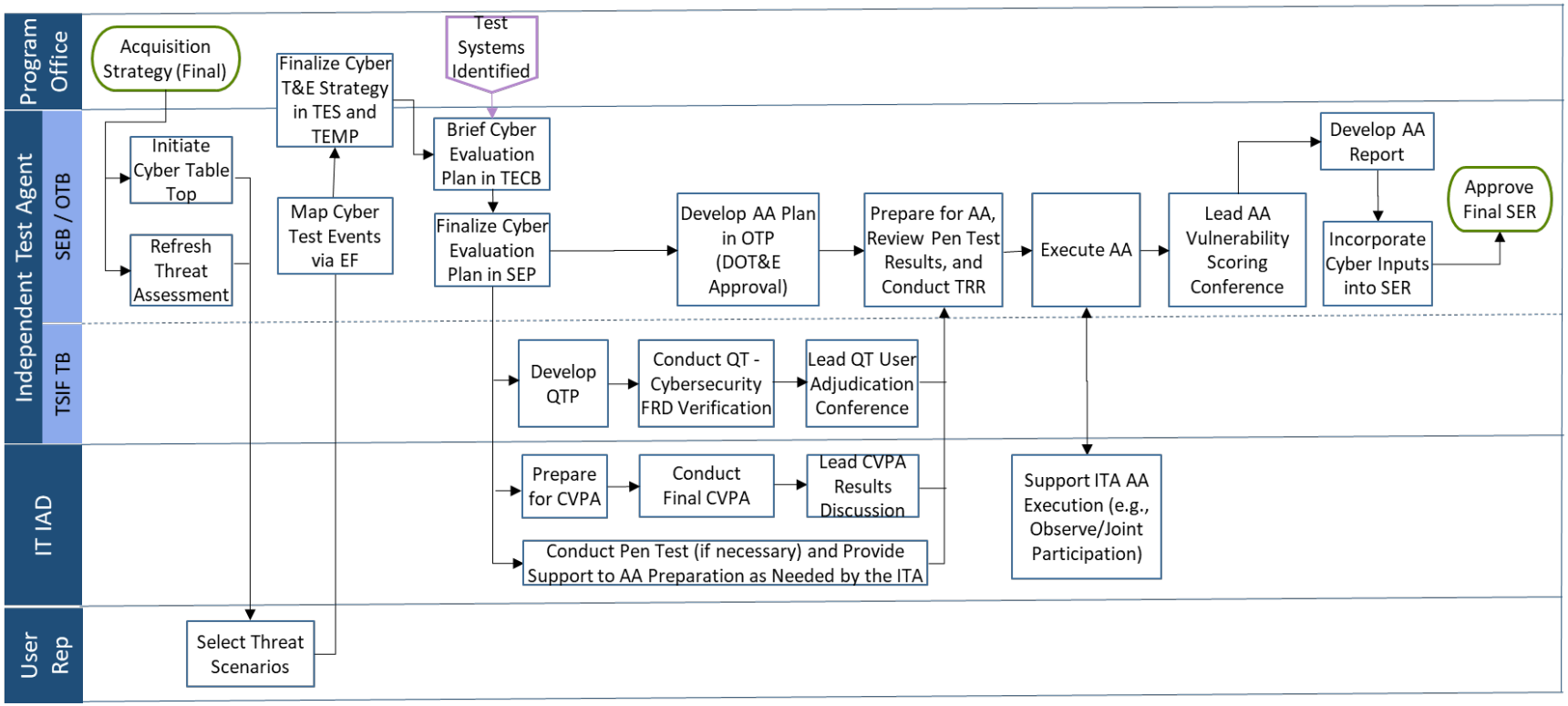
The objective of cybersecurity T&E early engagement with industry is to allow the vendor to fix any significant cybersecurity issues prior to delivery of the system for formal ITA evaluation. These events can be iterative, allowing for fix-test-fix cycles as the vendor hardens the system. Regardless of whether the cybersecurity T&E is performed by the TSA T&E Division, IT IAD, or even directly by the vendor, the early T&E would increase the maturity of candidate systems, inform TSA's decision on whether to accept a

system's technical data package, and lower the risk of unexpected cyber resilience deficiencies during the ITA's formal cyber resilience assessment.

D.4 Cybersecurity Test and Evaluation Strategy, Planning, Execution, and Reporting

The cybersecurity T&E lifecycle, from test strategy through reporting, is illustrated in **Figure D-2** and further described in the subsections that follow. Note: The purple shield end object in **Figure D-1** is depicted as an input in **Figure D-2** as illustrated.

Figure D-2: Cybersecurity T&E Strategy, Planning, Execution, and Reporting



D.4.1 Cybersecurity Test and Evaluation Strategy

The Requirements Sponsor works with TSA Intelligence and Analysis/Intelligence Analysis Branch to develop and/or refresh a general, aviation security threat assessment and with the IT/IAD Focused Operations Branch to develop the system-specific threat assessment. The threat assessment is developed and delivered to the ITA, program office, and User Representative during Test and Evaluation Master Plan (TEMP) development. The threat assessment provides a reporting of past and current threats to the system, likely adversaries, and their capabilities.

Leveraging threat assessment inputs, the ITA convenes a Cyber Table-Top (CTT) exercise to document the adversary scenarios/methods for exploiting the system. During the CTT, stakeholders from intelligence groups, IT, the program office, user representative, and the ITA document the various system interfaces, and the methods a threat actor may take to exploit those interfaces. Personnel with intimate system knowledge should be present at these sessions in order to ensure both cybersecurity and system-specific expertise are available.

The User Representative reviews the threat assessment and CTT outputs and selects their primary adversary threat scenarios. These scenarios indicate the highest risk scenarios from the User Representative's viewpoint and forms the basis for AA planning, execution, and reporting. A CTT extract is included in the TEMP and T&E Strategy (TES) Briefing to DOT&E. Additionally, in the TEMP and TES, the program office and ITA discuss the test strategy required to assess the adversary scenarios and complete the Cyber Resilience evaluation.

D.4.2 Cybersecurity Test Planning

Working with the OTD, the ITA Cybersecurity Test Team develops the AA Plan and incorporates the content within the Operational Test Plan (OTP). IT/IAD and/or the TTB may also develop a CVPA plan if a CVPA is required.

The AA Plan aligns with the adversary threat scenarios and other relevant content (e.g., measures, environment) in the TEMP. The AA Plan emphasizes an attack path based execution methodology where successful attacks are scored in their entirety during a post-test scoring conference. The scoring emphasizes the likelihood and mission impact of each successful attack path considering the operational environment and primary threat adversary (e.g., insider threat) as listed in the TEMP.

The AA Plan documents test team roles, responsibilities, activity timelines, and reporting artifacts to expect once activities are executed. The AA plan includes the test methodology required to attempt execution of each adversary scenario and is written in an operational/mission-oriented manner. The test team should utilize the system post-exploit, to understand the mission impact of vulnerabilities. For example, the test team may find that they can gain access to system files, however, are unable to modify/edit these files in such a manner as to negatively impact system performance. Any vulnerabilities, and their impact, should be documented in an operational manner (e.g., by altering configuration file, alarm disabled allowing adversary to potentially penetrate the checkpoint with an explosive device).

D.4.3 Cybersecurity Test Execution

In the weeks leading up to the start of testing, it is imperative for the Cybersecurity Test Team to complete necessary preparation items. These items include but are not limited to obtaining and reviewing vendor system documentation and manuals, obtaining accounts and passwords, establishing a point of contact list and protocols for contacting the vendor in case of system downing, reviewing organizational rules of engagement to mitigate the impact of system failure, and administrative items such as gaining access to the facility (e.g., badging or escorts).

The OTD convenes a Test Readiness Review (TRR) with the support of Cybersecurity Test Team within seven days prior to the start of testing. During the TRR, the test team will document status against predefined readiness criteria checklist to include a signed OTP and completion of all necessary preparation items.

During AA execution, the test team should provide a short, daily status reports documenting progress against planned completion dates, any risks or unexpected events, and a high-level activity summary. While the emphasis is execution against the plan, the test team can veer from the predefined test scripts/adversary scenarios as potential vulnerabilities and exploits present themselves. Any vulnerabilities outside of these predefined scenarios are valid findings and should be analyzed and reported as such. The team should not discuss any vulnerabilities or preliminary results in its regular status reports to avoid stakeholders forming incorrect conclusions on the overall evaluation.

D.4.4 Cybersecurity Analysis and Reporting

The OTD will conduct a vulnerability scoring conference with the System Evaluator approximately one week after the end of the AA and includes the program office, User Representative, and IT/IAD. The Cybersecurity Test Team will present each successful attack path, to include the individual vulnerabilities with photographs that were leveraged to execute the path, and assigns an initial impact and likelihood rating in alignment with the scoring methodology from the OTP. For each attack path, the team includes supporting information that will be relevant to the discussion of execution likelihood to include sophistication of attack (e.g., number of resources required), time required to execute by the likely attacker (e.g., insider threat), where the attack would take place, and whether any queues or triggers would result from the aviation security operational environment in the process.

The System Evaluator is the chair of the vulnerability scoring conference and ultimate decision maker for vulnerability scoring. The System Evaluator should consider the mission-based impact, kill-chain sophistication based on likely adversaries, and whether operational environment safeguards (e.g., SOC, SOP) mitigate the threat in determining the final score for each vulnerability.

The Cybersecurity Test Team works with the System Evaluator to produce an AA Report documenting the results of the AA. The System Evaluator will leverage the AA results with findings from the CVPA and QT cybersecurity FRD verification when determining whether the Cyber Resilience criteria is met. To be operationally cyber resilient, the system must remain effective and suitable to satisfy the mission while under duress from offensive cyber-attacks. The System Evaluator documents successful, and unsuccessful, attack attempts, with associated scoring, in the System Evaluation Report (SER).

D.4.5 Post Evaluation Activities

The System Evaluator and Cybersecurity Test Team will support the Program Office (if requested) with any discussion of test findings in Acquisition Review Board meetings, vendor Technical Interchange Meeting, or other such forums. The ITA may attend ongoing Plan of Action and Milestone meetings as required to track the status of deficiency remediation. The ITA's purpose in these meetings is to be prepared for any subsequent regression test activity. If required, the ITA may also be requested by the program office to conduct regression testing upon vendor submission of a change package in accordance with Section 3.8 of this Guidebook.

APPENDIX E: DOCUMENTATION GUIDELINES

Document	Lead Organization	Approval Authority	Approval Date (No Later Than)
Evaluation Strategy and Planning			
Early Strategy Review	System Evaluation Branch (SEB)	Executive Director, Independent Test Agent (ITA)	21 calendar days prior to the Test and Evaluation Strategy (TES) Briefing
TES Briefing	Program Management Office (PMO)	Director, Office of Test and Evaluation (DOT&E)	90 calendar days prior to Test and Evaluation Master Plan DOT&E submission
TEMP	PMO	DOT&E	30 calendar days prior to Acquisition Decision Event (ADE) 2A.
Test and Evaluation Concept Briefing (TECB)	SEB	DOT&E	120 calendar days prior to the start of Operational Test and 60 calendar days prior to Operational Test Plan (OTP) submission.
System Evaluation Plan (SEP)	SEB	Executive Director, ITA	After TECB approval and prior to OTP submission to DOT&E.
Determination of Test Scope (DTS)	SEB	Executive Director, ITA	21 calendar days after Tier 3 designation. Tier 3 designation to occur 7 calendar days after change package approval.
Test Event Planning			
Certification Test Plan (CTP)	Designated Government Certification Agent (DGCA)	Executive Director, ITA	30 calendar days prior to first day of test
Qualification Test Plan (QTP)	Transportation Security Administration Systems Integration Facility (TSIF) Test Branch	Executive Director, ITA	30 calendar days prior to first day of test
Operational Test Plan (OTP)	OTB	DOT&E	Submit for approval 60 calendar days prior to start of Operational Test

Document	Lead Organization	Approval Authority	Approval Date (No Later Than)
Operational Assessment (OA) Plan	OTB	OTB Manager or Executive Director, ITA if data will be a primary data source in a System Evaluation Report (SER).	14 calendar days prior to first day of test
Operational Utility Evaluation (OUE) Plan	OTB	OTB Manager	14 calendar days prior to first day of test
Acceptance Test Event Planning			
Verification and Validation Requirements Traceability Matrix (RTM)	PMO Engineering (P) RCA RDB T&E Division	PMO	Per vendor contractual deliverables
First Article Test and Evaluation (FAT&E) Plan and Procedures	PMO VRTM TSE Vendor author (P) ATSA –Acceptance Test Team Input	Acceptance Test Director	Per vendor contractual deliverables
Factory Acceptance Test (FAT) Plan and Procedures	PMO VRTM TSE Vendor author (P) ATSA – Acceptance Test Team Input	Acceptance Test Director	Per vendor contractual deliverables
Site Acceptance Test (SAT) / ORT Plan and Procedures	PMO VRTM TSE Vendor author ATSA – Acceptance Test Team Input	Acceptance Test Director	Per vendor contractual deliverables
Network Throughput Test (NTT) Plan and Procedures	PMO VRTM TSE Vendor author ATSA – Acceptance Test Team Approval	Acceptance Test Director	Per vendor contractual deliverables
Integrated Site Acceptance Test (ISAT) Plan and Procedures	PMO VRTM TSE Vendor author ATSA –Acceptance Test Team Approval	Integrated Acceptance Test Director	Per vendor contractual deliverables

Document	Lead Organization	Approval Authority	Approval Date (No Later Than)
Evaluation Reporting			
SER	SEB	Executive Director, ITA	45 calendar days prior to ADE-3. 45 calendar days after the final Data Authentication Group (DAG)
SER Communication Memorandum	SEB	Executive Director, ITA	7 calendar days after SER approval.
Letter of Assessment (LOA)	DOT&E	DOT&E	30 calendar days after SER submission date to DOT&E
Test Event Reporting			
Certification Test Report (CTR)	DGCA	Director, DGCA	45 calendar days after the last day of test
QT Report (QTR)	TSIF Test Branch (TTB)	Manager, TTB	45 business days after the final DAG
QT Final Results Summary (FRS)	TTB	Manager, TTB	15 business days after the final DAG
QT Quick Look Report (QLR)	TTB	Manager, TTB	15 business days after the final DAG
Data Collection Activity Report	TTB	Manager, TTB	45 business days after the final DAG
Cooperative Vulnerability and Penetration Assessment QLR	TTB	Manager, TTB	15 business days after the end of test
Adversarial Assessment Report	OTB	Manager, SEB	30 calendar days after the vulnerability scoring conference
OA Report	SEB	Manager, SEB	45 calendar days after the final DAG
Emerging Results Briefing (Post-OT)	OTB	Executive Director, ITA	30 calendar days after the last day of test
OT/OA Quick Look Report (QLR)	SEB	Manager, SEB	10 calendar days after the final DAG

Document	Lead Organization	Approval Authority	Approval Date (No Later Than)
OUE Report	SEB	Manager, SEB or Executive Director, ITA if data used as a primary data source in a SER.	45 calendar days after the final DAG
Acceptance Test Event Reporting			
FAT&E Report	TSE Vendor ATSA Observations	PMO, ATSA, TSIF Test Team	14 calendar days after the Test
FAT Report	ATSA	Manager, ATSA Branch	14 calendar days after the Test
SAT / ORT Report	ATSA	Manager, ATSA Branch	14 calendar days after the Test *ORT is the same scope as SAT; however, a SAT is for initial install and ORT is for any major changes since SAT
NTT Report	ATSA	Manager, ATSA Branch	14 calendar days after the Test
ISAT Quick Look Report QLR	ATSA	Manager, ATSA Branch	14 calendar days after the Test
ISAT Test Report	ATSA	Manager, ATSA Branch	45 calendar days after the Test
BASE Airport CBIS Report	ATSA – BASE Team	Manager, ATSA Branch	Per Deployment and Sustainment Division Request

APPENDIX F: TEST AND EVALUATION ROLES AND RESPONSIBILITIES

The roles and responsibility matrix **Table F-2** outlines the **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed (RACI) entities for Test and Evaluation (T&E) deliverables. **Table F-1** provides a key.

Table F-1: T&E Deliverable Routing Definition of Terms

Role	Denoted By	Description
Responsible	R	Does the work to complete the task. Escalates issues to accountable party as appropriate.
Accountable	A	Ultimately answerable for the completion of the task. Assigns responsible party to the task.
Consulted	C	Active participant who may provide input to the task completion. Input occurs by contributing to the development of the document or via review and comment periods, formal routing, signature marking concurrence, etc.
Informed	I	Participants kept informed as needed and may be provided the final deliverable upon completion. Input not necessary for task completion.

Table F-2: T&E Deliverable Roles and Responsibilities

R	Responsible
A	Accountable
C	Consulted
I	Informed

	Core T&E Leadership				Core T&E Team					Sub Team			
	SEB Manager	TSL IT&E Test Director	TTB Manager	OTB Manager	System Evaluator	TSL IT&E Test Lead	QTD	OTD	T&E Manager	Project Manager	User Representative	IT IAD	DOT&E Portfolio Lead
Planning													
Early Strategy Review	A	C	C	C	R	C	C	C	R	A	C	C	I
Test and Evaluation Strategy Briefing	C	C	C	C	R	C	C	C	R	A	C	C	C
Test and Evaluation Master Plan	C	C	C	C	R	C	C	C	R	A	C	C	C
Test and Evaluation Concept Briefing	A	C	C	C	R	C	C	C	C	C	C	C	C
System Evaluation Plan	A	C	C	C	R	C	C	C	C	I	I	C	I
Determination of Test Scope	A	C	C	C	R	C	C	C	C	I	I	C	I
Certification Test (CERT) Plan	I	A	I	I	C	R	I	I	I	I	I	I	I
Qualification Test (QT) Plan	I	I	A	I	C	I	R	I	I	I	I	I	I
Operational Assessment (OA) Plan	C	I	I	A	C	I	I	R	C	I	I	I	I
Operational Test (OT) Plan	C	I	I	A	C	I	I	R	C	I	I	I	C
Data Collection Activity Plan (TSIF)*	I	I	A	I	I	I	R	I	I	I	C	I	I
Operational Utility Evaluation Plan*	C	I	I	A	C	I	I	R	I	I	C	I	I
Execution													
QT Status Reports	I	I	A	I	I	I	R	I	I	I	I	I	I
OT Status Reporting	I	I	I	A	I	I	I	R	I	I	I	I	I
OT/OA Data Authentication Group	A	I	I	A	R	I	I	R	C	C	C	I	I
Reporting													
CERT Report	I	A	I	I	C	R	I	I	C	C	C	I	I
CERT Letter Concurrence Memo	A	I	I	I	R	C	I	I	I	I	I	I	I
QT Report / Final Results Summary	I	I	A	I	C	I	R	I	C	C	C	I	I
OA Report	A	I	I	C	R	I	I	C	C	C	C	I	I
OT/OA Quick Look Report	A	I	I	C	R	I	I	C	C	I	I	I	I
Emerging Results Briefing	C	I	I	A	C	I	I	R	C	I	I	I	C
Adversarial Assessment Report	A	I	I	C	R	I	I	C	C	C	C	C	C
System Evaluation Report (SER)	A	C	C	C	R	C	C	C	C	C	C	C	C
SER ITA Memo	A	I	I	I	R	I	I	I	I	I	I	I	I
Data Collection Activity Report (TSIF)*	I	I	A	I	C	I	R	I	I	I	I	I	I
Operational Utility Evaluation Report*	A	I	I	C	R	I	I	C	I	I	C	I	I

*Roles and responsibilities may vary.

The document routing roles and responsibility matrix (Table F-4) outlines the parties responsible for T&E document routing, concurrence, and approval. **Table F-3** provides a key.

Table F-3: Document Routing Definition of Terms

Role	Denoted By	Description
Originate	O	Initiates the formal routing of a document.
Review and Concur	R	Receives an opportunity for review, comment, and concurrence during formal routing of a document.
Consulted	C	Active participant who may provide input to the task completion. Input occurs by contributing to the development of the document or via review and comment periods, formal routing, signature marking concurrence, etc.
Informed	I	Participants kept informed as needed and may be provided the final deliverable upon completion. Input not necessary for task completion.

Table F-4: Document Routing Roles and Responsibilities

	Core T&E Leadership						Core T&E Team					Sub Team				
O Originate R Review and Concur C Concur and Sign A Approve and Sign Not Delegated / Delegated	Executive Director, ITA	Deputy Director, ITA	SEB Manager	TSL IT&E Test Director	TSIF Test Branch Manager	OTB Manager	System Evaluator	TSL IT&E Test Lead	QTD	OTD	T&E Manager	Component Acquisition Executive	Executive Director, PEO	Project Manager	User Representative	Director, Office of Test and Evaluation
Planning																
Early Strategy Review	A	R	R				O	R	R	R	O		A	O		
Test and Evaluation Strategy Briefing	R	R	R			R	R	R	R	R	O	-/A	R	O	R	A/-
Test and Evaluation Master Plan	C	R	R		R	R	R	R	R	R	O	C/A	C	O	C	A/-
Test and Evaluation Concept Briefing	R/A	R	R		R	R	O	R	R	R					R	A/-
System Evaluation Plan	A	R	R		R	R	O	R	R	R					R	
Determination of Test Scope	A	R	R			R	O	R	R	R						
Certification Test (CERT) Plan	A	R		R			R	O								
Qualification Test (QT) Plan	A	R			R		R		O							
Operational Assessment (OA) Plan			R			A	R			O						
Operational Test (OT) Plan	C/A	R	R			R	R			O					R	A/-
Data Collection Activity Plan (TSIF)*			A						O							
Operational Utility Evaluation Plan*						A	R			O						
Reporting																
CERT Report				A			R	O								
CERT Letter Concurrence Memo	A	R	R				O									
QT Report / Final Results Summary					A		R		O							
OA Report			A			R	O									
OT/OA Quick Look Report			A			R	O									
Emerging Results Briefing	R/-	R/-	R/-			R/-	R/-			I/-						A/-
Adversarial Assessment Report			A			R	O			R						
System Evaluation Report (SER)	A	R	R	R	R	R	O	R	R	R						
SER ITA Memo	A	R	R				O									
Data Collection Activity Report (TSIF)*					A				O							
Operational Utility Evaluation Report*			A			R	O			R						

*Roles and responsibilities may vary.