Developmental Testing and Evaluation (DT&E) Designation Test Plan Template

Office of SAFETY Act Implementation

March 2023

Science and Technology

Contents:

The goal of a test or pilot deployment conducted during a Developmental Testing and Evaluation (DT&E) Designation is to collect information about the performance of the Technology[1] in its intended operating environment and to learn about the specific anti-terrorism capabilities of that Technology as presented in the associated application for Designation protection. SAFETY Act applicants should consider what testing is appropriate for their Technology, particularly as related to performance metrics, test conditions, test numbers, and the validity of test scenarios. The goal of the test plan is to help both you and the Office of SAFETY Act Implementation (OSAI) understand what types of information to expect in a full Designation application.

You will use your test plan to collect quantitative and qualitative data to support the performance of your Technology. Your test plan could also include the collection of customer or user surveys, the finalization of process and procedural documentation, or the specification of lessons learned and follow-on corrective actions. The data and information collected through the test would then be used to support a future SAFETY Act Designation application. Test plans can be developed for all types of anti-terrorism technologies (ATTs) and are customized based on the Technology and its intended mission or use case.[2] The type of testing and data should be unique to the Technology. While the type of data collected is paramount, the environment and conditions of the test in which that data are collected are also important. For example, for security controls that are vulnerable to malicious disruption, such as cyberattacks, effectiveness can be supported by providing data results from testing the security controls. Test plans should consider collecting this type of data to support a full Designation evaluation.

This guide describes the major sections of a test plan and briefly discusses what OSAI suggests should be included in those sections. OSAI is providing this template as a helpful resource, its use is not required. Again, you should tailor your test plan document to your specific Technology and use case.

1. Introduction

Provide any introductory remarks to set the stage for your test. This is a good section for an overview of your Technology and a description of the general mission or use case.

2. Purpose

Describe the Technology, its intended mission, and example scenarios, use cases, or applications that match a typical deployment. Identify critical dependencies[3] that may affect the performance of your Technology. Examples include the skills and experience of users and pre-existing infrastructure needed to properly employ your Technology. Your description may include the

[1] In this document, "Technology" refers to what you are seeking SAFETY Act protection for – it could be a system of systems, a piece of equipment, etc.

[2] A use case is the specific situation in which a product or service could potentially be used, such as at a stadium, an airport, etc.

[3] A critical dependency is a reliance on third-party products and services such that the loss of one or more suppliers results in disruption that would preclude the delivery or operation of the Technology.

application of proper protections hardware, information technology (IT), or services. A proper description should at least answer the following questions:

- What is the name of your Technology?
- What type of customer is the primary user for your Technology?
- Have any of your customers or potential customers requested your Technology have SAFETY Act protections as a condition of procuring it?
- What is the primary mission or function of your Technology?
- What types of acts of terrorism is your Technology intended to counter (e.g., deterrence, prevention, mitigation, response, recovery)?
- Where is your Technology most frequently deployed?

A. Approach

Describe how and where testing will be conducted (including the operational environment[4]), dependencies such as external data sources, and parties responsible for conducting the test (including their particular expertise).

Identify the stakeholders and sign-off authorities.

Outline the phases of the testing program, if applicable, with objectives, capabilities to be assessed, and expected outcomes and reports.

Discuss, in detail, any limitations affecting the test's completion, such as resources, locations, or availability of trained personnel, and your plan(s) to mitigate these limitations.

Outline the testing approach for critical dependencies – such as cybersecurity protections, third-party suppliers or services, external information sources, and so forth – if these are essential for your Technology's effectiveness. Examples of questions to answer include:

- What components of your Technology will you be evaluating in the test period?
- Is this a full or partial test of your Technology (e.g., component testing versus integrated system testing, limited-scope tests, specific subset or whole range of services, etc.)?
- What is your setting for the test or pilot deployments (type of customer(s), market sector(s), deployment locations, venues, etc.)?
- How many locations will be included in your test?
- How many personnel will be involved in your test (participants, testers, supervisors)?
- How long will the test be (number of months, years, or, alternatively, number of events)?
- What questions do you hope to answer with this test? What do you hope to learn?
- What are the goal and purpose of the test?
    - Are you assessing performance in an operational environment?
    - Are you assessing specific procedures with an aim to improve?

[4] In general, the operational environment refers to the conditions, influences, and circumstances that would impact the deployment of a Technology in a live setting. It includes, for example, environmental factors such as heat, humidity, noise, etc. that could influence a Technology's performance.

- Are you assessing training materials and users' or operators' understanding of those materials?
- Are you assessing a quality management program?

B. Strategies

Describe how the test will address the Technology (all components if needed), including its critical dependencies. Also describe how the scenarios, locations, participants, data, and other elements were chosen to support the test objectives of simulating a real-world operational environment to the extent possible.

If the test program does not test some aspects of the Technology, or if some components are being tested separately or differently, please describe those strategies as well. Since the proposed testing may not be sufficient to assess all aspects of your Technology, the purpose here is to outline what subset of functional or technical components you selected and how they are representative of real-world deployments. Questions to consider include:

- What is the scenario(s) for your test?
  - Are you assessing routine procedures and operations, emergency operations, normal or high levels of workload, etc.?
  - Are you looking at performance in different environments or locations?
- How many test phases or smaller component tests do you plan?
- How did you select this scenario?
- Do you plan intermediate reviews of your test progress or data collection?
- Do you have a procedure or plan to stop the test early, if necessary?
  - Who is involved in deciding to stop or pause the test?
  - How do you determine the criteria or conditions that must be met to resume your test?

C. Logistics

Describe your expected test deployments. Clearly state what you will provide and what your customer or user will provide to support the test. For example, discuss the computing and physical deployment environments. Are you supplying a network for testing software or are you testing on a customer network? Is your customer providing power and water?

Outline the number of test phases with configuration(s), participating personnel and job positions, locations, data intake variations, false positive/false negative scenarios, and so forth. Identify key assumptions such as availability of specific environment configurations, data, and personnel to complete the test program.

Outline the overall logistics management[5] for the test program and all the events during its execution. In doing so, you should consider things such as:

- Materials, equipment, and supplies (supply chain for availability of spares, consumables).
- Technology (test equipment, maintenance equipment, servers, hardware).
- Data (access to external data repositories and data reduction capabilities, facilities information, and other data libraries).
- Personnel and third-party services and training.
- Documentation (procedures and requisite supplemental manuals).

Also, consider the following questions:

- Will you change the environment conditions during the test, or between tests? If so, how?
- What are the jobs of personnel who will participate in your testing (supervisors, test managers, test operators, customers, independent test agencies, government personnel, data analysts, test observers, instructors or trainers, etc.)?

D. Metrics

Describe what you will measure during the test and how those measures will help you determine the Technology's effectiveness. Also, identify why the testing is being performed, including specific references to associated SAFETY Act Designation Criteria and other formal requirements. Outline objectives and what constitutes acceptance for the testing as a whole. To the extent possible, test metrics should be quantitative and measurable, but they may be qualitative where necessary. Test metrics should be based on data (quantitative or qualitative) that demonstrate acceptable performance as specified by formal acceptance criteria. These criteria should align with your Technology Description and your Technology's capabilities.

E. Deliverables

Describe what results are anticipated and how they will be documented. Also describe what will be evaluated in the test report.

- Do you expect to update any components or procedures of the Technology during or after the test?
- Do you expect any of your documentation (policies, procedures, training, manuals, release notes, etc.) to be updated, revised, or changed as a result of the test?
- Will you publish after-action reports? If so, what information will you include in them?
- Do you expect any external or third-party agencies to report on or assess the test and your Technology?

[5] In this case, logistics management refers to ensuring that all the necessary test equipment, personnel, and supporting resources are available for the test.

Test reports can and should vary according to the nature of your Technology, deployment scenario, environment, and type of testing. Table 1 outlines the major portions of a typical test report.

Table 1. General Test Report Sections

Section Title	Contents
Executive Summary	The executive summary provides a short synopsis of the testing to be performed in the context of your overall DT&E Designation testing program, as described in your test plan. Include the testing objectives and outline the test methodology. Then, briefly summarize the results, emphasizing performance relative to defined acceptance criteria. Discuss whether you needed to make any changes from your plan and whether you needed to pause your testing. Highlight the consequences of any significant variance from desired results. Outline next steps as appropriate.
Detailed Test Report Summary	The detailed test report summary is a narrative with supporting tables, graphs, incident records, and other exhibits. The summary should contain results that relate to the metrics described in the test plan. Include explanations that help a layperson understand the results. Explain the relationship of the results to the acceptance criteria. Describe whether the test's goal, mission, or target was achieved, and describe the aggregate performance of the Technology and the degree of variance in that performance.
Test Variance	This section notes any variations from the original test plan or acceptance criteria. This is especially important since OSAI has accepted your test plan as part of your DT&E Designation award. Document the changes from the test plan or concept and the impact of those changes. Describe any alternative testing you conducted. Also describe next steps, especially required corrective actions and future testing.
Approval	This section contains the formal approval block or a notification of test failure.

3. Previous Testing

Provide information on any previous testing and other relevant information that affects your DT&E Designation test plan. For example, provide information on any laboratory testing; proof-of-concept, prototype, or component testing; environmental testing; third-party agent testing; etc., that you have conducted. Information should be in the form of test reports, if available. If extensive testing has been conducted, information can be in the form of a narrative overview, with supporting attachments or references.

4. Individual Test or Test Collection Description

A. Mission

State the mission of the test(s) (i.e., the goal of your test). Describe how the test will be performed, explain how testers or users will identify and report defects, and explain how you will implement fixes.

- What is, and what is not, being tested relative to your Technology Description and why?
- What is the mission of the Technology or the services?
- What is the goal or aim of the test?
- What do you want to improve or understand after the test or pilot deployment?

B. Management

For the test program as a whole, discuss your logistic processes for tests and any other events occurring during deployment. Discuss the roles, responsibilities, and qualifications of key personnel and organizations, including:

- Seller(s);
- User(s);
- Third parties;
- Test team manager (required) and members;
- Key support personnel;
- Reviewers and approvers; and
- Others.

C. Configuration

1. Technology Configuration Management

Configuration management refers to how you document your requirements and changes to those requirements through the life of your test. The following items will help you capture that information.

Describe the planned configuration of the Technology for the test and logistics for the test. For the purposes of a SAFETY Act DT&E Designation, the baseline Technology configuration is your SAFETY Act Technology Description. If you have not written your Technology Description, you should do so before drafting your test plan.

- Describe how configuration management will be maintained. In other words, how will you ensure the test system remains representative throughout testing?
- Identify variations from the standard Technology configuration. Also, identify components of the Technology being tested, components not being tested, and variations (i.e., deviations or exclusions from your Technology Description). Explain how potential deployment or test locations may vary for each deployment test location.

- Define your process for background screening or vetting of the personnel participating in or managing the test.
- Discuss the minimum levels of training and any variances in training for different job positions for personnel participating in the test.
  - How are you training your personnel?
  - Are your personnel licensed to any Federal, State, or local standards or to any professional qualifications?

2. Facts, Assumptions, Constraints, Limitations, Prerequisites, and Contingencies

Identify items or circumstances that impact the Technology and the assumptions you are making with respect to the Technology. This includes approved acceptance criteria; preliminary and exploratory tests; successful tests of critical support systems and functions; availability of inputs; availability of skilled staff, analytical tools, and third parties; and defined and documented policies and procedures.

- Do you have any constraints for your tests?
- Have you identified unavoidable limitations in your test plan?
- Do you have prerequisites for your tests?
- What are the risks to your test based on the availability of locations, environments, or supplies?
  - What is your process for identifying these risks?
  - What is your risk mitigation plan? How will you manage the risks to the tests?
  - Are there potential financial risks that could affect the completion or conduct of the tests?
- Describe the staging and acceptable state of data, other inputs, and measurement processes and technologies needed for the Technology to perform its task.
- Describe how tests or deployments are representative of the Technology Description and real-world scenarios.
- Describe any deviations from the Technology Description (component testing versus integrated system testing, limited-scope tests, prototype, etc.).
- Discuss the process and technology that will be used to validate testing was performed sufficiently and describe the actions required if failures in test execution occur.
- Identify conditions for temporary suspension (or termination, if any) of testing and the criteria for resumption. These conditions could be excess false alarms or false positives, equipment failure, insufficient staffing, safety concerns, data collection errors, etc.

D. Safety

Identify how you plan to ensure the safety of the public and your employees during tests or deployments. In addition to occupational safety risks, describe any other (e.g., environmental, financial) potential risks and how they will be managed during the course of a test or deployment.

- Provide a safety plan if required and applicable.
- Describe how you will communicate your safety plan or train your personnel prior to testing.

E. Supporting Information and Documentation

Provide additional documents to support your Technology and test plan.

- Identify applicable Federal, State, and local supporting regulations, standards, specifications, guidelines, etc. In particular, identify those that provide test requirements for your Technology.
- Identify and describe all licensing and certifications required for deployment. For example, discuss any safety certifications, environmental approvals, inspections, or regulatory compliances needed.
- Provide the above information for dependent systems critical to your test.
- Provide supporting information (supplementary exhibits) applicable to your test, such as standard operating procedures, operations and maintenance manuals, user operating manuals, training manuals, and drawings (deployment layout, IT architecture).

5. Test Deployments

A. Schedule for Testing or Pilot Deployments

Include the test schedule. Also include the following information:

- Number of deployments.
- Duration of each deployment.
- Total duration of the test.
- Confirmation that deployment locations have agreed to host testing.
- The physical address of each deployment location or test location.
- A point of contact (POC) for the test.

Consider completing Table 2.

Table 2. POC Information

POC Name	Position	Email	Phone

B. Test Environment, Implementation, and Maintenance

Describe the environment, location, and implementation of your test events. Include your communications and maintenance plans, personnel, and users and any plans to monitor and record incidents, deficiencies, bugs, faults, failures, or other problems.

- Describe your company's and employees' participation in the testing. Will you be conducting the testing or providing oversight? Will you provide maintenance or technical support? Will you provide on-site or on-call maintenance personnel?
- Identify other parties that will participate in testing, particularly U.S. Federal Government or military entities.
- What is your communications plan for the test(s)?
  - What are your procedures to escalate test problems to supervisors or test managers?
  - What is the decision process to stop or resume testing?
  - Who has primary responsibility for deciding to stop the test?
  - Who has the responsibility for changing the conditions of the test?
- What type of incident or problem-tracking process are you using?
  - What type of information will be collected for incidents or problems?
  - How will you track your corrective actions or responses to incidents?
- Discuss your users.
  - Describe the users at the deployment location.
  - Describe how the users will employ the Technology.
  - Describe the users' capabilities and training.
  - Describe any training provided to the users.

C. Ancillary Services and Required Processes

Identify any dependent or third-party sources (e.g., products, IT, services) required for deploying your Technology.

D. Objective/Test Requirements

Both products and services should have specific test objectives or requirements. These set goals you would like to achieve or your metrics for the test at large. What would you like to learn in the test? For products, these objectives or requirements commonly are in the form of key performance indicators or quantitative measures. Clearly listing these indicators in a table that includes a rationale for that objective or requirement can be helpful. Service technologies could have similar quantitative (e.g., response time or training compliance) or qualitative (e.g., general incident categorization or customer satisfaction) measures.

E. Data Recording

State who and how you will record your data. You can always include sample test record sheets as an appendix to your test plan.

6. Test Reporting Support Processes

This pertains to roles, processes, and technologies needed for reporting test progress, test failures, deficiencies discovered during testing, and other information required to identify testing or technology improvements. Processes and technologies should let you record and retrieve

changes in testing data and activities throughout the test program. Document management decisions that resulted in changes to the test plans or changes to the Technology.

Glossary

Act of Terrorism	As the term is defined in the SAFETY Act of 2002 at 6 U.S.C. 444(2) and the Regulations Implementing the SAFETY Act at 6 C.F.R. §25.2
Assumptions	Conditions necessary for testing about which incomplete or unobtainable knowledge exists but which are assumed to be true; suppositions about the current or future developmental testing and evaluation that are assumed to be true in the absence of facts adjudicated by qualitative or quantitative data (*adapted from Field Manual 101-5, U.S. Army*)
Availability	Metric that the Technology has not failed, is not undergoing a repair action, or otherwise has not been capable of providing specified functions, expressed in the context of defined performance criteria
Capabilities	The collection of activities, functions, features, physical systems, skills, knowledge bases, and managerial systems that create a special anti-terrorism advantage as defined in the Technology Description
Configuration	The particular combination of Technology activities, functions, features, physical systems, software, and supporting services associated with a particular test or collection of tests
Configuration Management	Change control process consisting of written policies and procedures to validate and document changes to Technology features, functions, and other components defined in the Technology Description
Constraints	Formally defined and documented limitations or restrictions on the scope of test execution
Contingencies	Formally documented section of a test plan that identifies the overall risks to test execution, the events associated with these risks, the actions to be implemented if one or more of the identified events occur, and the conditions upon which testing will be terminated
Facts	Statements of known data concerning the situation, including, but not limited to, test parameters, strengths and weaknesses of the technology used, and material supplies available (*adapted from Field Manual 101-5, U.S. Army*)
Integrity	(1) The Technology performs its intended functions without being degraded or impaired by changes or disruptions in its internal or external environments (2) Test results are accurate and consistent and have not been altered or otherwise manipulated
Limitations	Actions generally prohibited by funding, higher authority, or technological advancement that influence the test manager's actions in

	developmental testing and evaluation (*adapted from Joint Publication 5-0, DoD*)
Logistics	Formally documented process of organizing and implementing all support required to execute one or more test plans, including materials, equipment, supplies, technology, data, personnel, and third-party services
Maintainability	Metric that the Technology's specified functions will be fully restored in a given time period, expressed in the context of defined performance criteria
Metrics	Standards of measurement that define the degree to which a Technology achieves a pre-defined capability or set of capabilities
Operational Effectiveness	The achievement of formally defined Technology performance objectives based on specified performance metrics in the intended operating environment with typical users
Prerequisites	Pre-specified conditions that have to be in place before executing one or more test plan elements
Qualified Anti-terrorism Technology	As defined in the SAFETY Act of 2002 at 6 U.S.C. § 444(1), "*any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated*" by the Under Secretary of Science and Technology and as set forth in the Regulations Implementing the SAFETY Act at 6 C.F.R. §25.2. Technologies that receive SAFETY Act Designation are considered qualified anti-terrorism technologies.
Qualitative	Non-numerical data that are descriptive and conceptual and can be categorized based on traits and characteristics
Quantitative	Numerical data that can be statistically and mathematically processed
Reliability	Metric that the Technology, including all supporting and dependent components, will satisfactorily perform the functions for which it was designed or intended, for a specified time and in a specified environment, expressed in the context of defined performance criteria
Responsiveness	The specific ability of the Technology as a whole or of specified components to complete assigned tasks within a specified time

SAFETY Act Designation Criteria	The criteria set forth in the SAFETY Act at 6 U.S.C. §441(b) and in the Regulations Implementing the SAFETY Act at 6 CFR 25.4(b). See also the Designation application for information on addressing these criteria in a full SAFETY Act Designation.
Test Plan	Documentation specifying the scope, approach, resources, and schedule of intended testing activities (*DHS Instruction 026-06-001 Test and Evaluation; DHS Instruction 102-01b*)
Test Report	Addresses critical issues observed during operational testing and evaluates the operational effectiveness and operational suitability of the system
Use Case	A list of actions or events defining the interactions between users (manual or Technology-generated events) and a system (the Technology) to achieve a goal