Department of Commerce • National Oceanic & Atmospheric Administration • National Weather Service

NATIONAL WEATHER SERVICE INSTRUCTION 80-305
April 8, 2009

Science and Technology

Systems Engineering

TEST AND EVALUATION

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/

OPR: W/OST3 D. Jones **Certified by:** W/OST1 J. C. Duh
Type of Issuance: Routine

SUMMARY OF REVISIONS: This directive supersedes NWS Instruction 80-305, dated October 28, 2004. Changes were made to (1) update the names of certification and approval officials to reflect the personnel changes; (2) change type of issuance from Initial to Routine and provide Summary of Revisions information; (3) update Section 1 to add phrases to clarify that the test results provide information to support decisions on commissioning/deployment, and not lead the decisions; (4) update Section 1 and 3.5 to include the security test and evaluation activities to verify the security controls and requirements; and (5) revise Appendix B and C to update definitions and references of NWS policy directives and instruction, and security policy.

SUMMARY: This instruction specifies the test and evaluation master plan template for all projects authorized under the Operations and Services Improvement Process (OSIP). Each program should establish and manage its test effort to ensure timely, efficient, and comprehensive data that support evaluation processes, and through effectively managed processes, lead to systematic improvement. Each program test and evaluation process must ensure, to the maximum extent possible, that the end item fulfills the established requirements and is operationally acceptable. To support this goal, this instruction specifies the template for a Test and Evaluation Master Plan (TEMP), and provides examples of Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) reports. This instruction relates to NWS Policy Directive 80-3 *Systems Engineering*.

signed March 25, 2009
Donald H. Berchoff Date
Director, Office of Science and Technology

Test and Evaluation

Table of Contents Page

Test and Evaluation

1. Introduction. Test and Evaluation (T&E) supports system engineering processes for Verification & Validation (V&V). Testing is a process of objective and repeatable use-based review of a system, subsystem, or component that is the basis for evaluation and judgment. The purpose of evaluation is to review, analyze, and assess data obtained from testing and other means to aid in making systematic decisions. The purpose of T&E is to verify technical performance, operational effectiveness, operational suitability, sustainability, system security, and to provide essential information to support decisions.

Developmental Test and Evaluation (DT&E) focuses on the verification of technical requirements primarily during the operational development phase. DT&E provides clarity about the system without introducing operational complexity, by controlling the test environment. DT&E is conducted by system developers and integrators. Tests performed as part of DT&E trace to the system requirements specification. Security testing activities are also included in the system DT&E.

Operational Test and Evaluation (OT&E) focuses on operational effectiveness and suitability, introducing realistic and actual operational considerations that may influence concepts of operation, requirements, design, and system use. OT&E includes testing in which varying degrees of the operational environment are introduced. It may include early operational assessment, operational assessment, initial operational test and evaluation, and follow-on operational test and evaluation. Representatives from the user and maintenance communities participate in operational testing. Tests performed as part of OT&E trace to operational requirements and test results provide information to support decisions on commissioning and/or national deployment of the system.

Security Test and Evaluation (ST&E) focuses on the verification of management, operational, and technical security controls that have been integrated into the system in response to business, functional, and other requirements of system performance. ST&E supports the certification and accreditation process, and provides the system owner, the certifying official, and the authorizing official with an overall evaluation of the system’s security posture, and the security risks associated with system operations. ST&E includes interviews with system development and operations personnel, examination of system documents, equipment, configurations, facilities, and other system components, and technical testing, to include vulnerability assessments, of system components and the integrated system. In some cases, penetration testing may be required. ST&E begins in the development phase, and should be integrated into the DT&E test plan so that security deficiencies can be noted and corrected prior to OT&E. Development ST&E may be accomplished by systems developers and integrators, and is used to identify security deficiencies that need correction prior to deployment, and security risks that may require acceptance by the authorizing official as a condition of operations. ST&E is also part of OT&E, and should be included in the OT&E plan. During OT&E security testing, the emphasis is on assuring the system will perform its operational functions in a secure manner commensurate with the level of security controls identified. Issues noted during DT&E security testing are reevaluated during OT&E security testing. Corrective actions are validated; issues not corrected are identified as system vulnerabilities and included in the system security risk analysis. OT&E security testing may be accomplished by the system owner, or may require an independent assessment, depending on the system's security categorization. ST&E costs are included in the system program plan and budget and the efforts are typically organized by the Information System Security Officer (ISSO).

2. Purpose and Scope. This instruction specifies the framework and functions that can be used for test and evaluation. Each program should establish and manage its test effort to ensure timely, efficient, and comprehensive data that support evaluation processes, and through effectively managed processes, lead to systematic improvement. The context, framework, and schedule for test and evaluation are shown in Appendix A, Figure 1.

3. Program Product Standards. This section defines the standard template for a Test and Evaluation Master Plan (TEMP), the guiding plan for a test and evaluation program. Table 1 below provides a summary of milestones associated with developing sections of the TEMP. The activities required to complete the TEMP will result in planning an appropriate test program to evaluate a system. Specific definitions supporting the information presented here are included in Appendix B.

Table 1. Summary of Milestones Associated with TEMP Sections

Test and Evaluation Master Plan Section	**Preliminary Version**	**Complete Version**
System Introduction	After Gate 3	Before Gate 4
Test and Evaluation Master Schedule and Management	After Gate 3	Before Gate 4
DT&E Plan	After Gate 3	Before Gate 4
OT&E Plan	After Gate 3	Before Gate 4
T&E Resource Summary	After Gate 3	Before Gate 4
Appendices	After Gate 3	Before Gate 4

3.1 System Introduction. Provide a summary of system objectives, measures of effectiveness and suitability, a system description, and an identification of critical technical parameters.

3.2 Test and Evaluation Master Schedule and Management. Provide an integrated test program schedule and description of the overall test and management process. This section should reference applicable test policies.

3.3 DT&E Plan. Provide an overview of the DT&E plan. Reference the Requirements

Specification and trace testing to system requirements. For complex projects and programs, the DT&E Plan may be a separate document that is referenced in this section. The DT&E Plan will include the following:

- Background
- Purpose and objectives
- System under test description
- Test cases
- Use cases
- Assumptions and limitations of the test and system under test
- Applicable policies
- Test management
- Entrance criteria
- Success criteria
- Test schedule
- Planned test report(s). (An example is provided in Table 2.)

3.4 OT&E Plan. Provide an overview of the OT&E plan. Reference the Concept of Operations / Operational Requirements Document (ConOps/ORD) and trace testing to operational requirements. For complex projects and programs, the OT&E Plan may be a separate document that is referenced in this section. The OT&E Plan will include the following:

- Background
- Purpose and objectives
- System under test description
- Assumptions and limitations of the test and system under test
- Applicable policies
- Test management
- Entrance criteria (including completed DT&E with test report)
- Success criteria
- Test schedule
- Planned test report(s). (An example is provided in Table 3.)

3.5 T&E Resource Summary. Identify the necessary physical resources and activity responsibilities. The following items may be included: test articles, test sites, test instrumentation, test support equipment, test targets and other expendables, operational force test support, simulations, models, test data, test-beds, information security safeguards, special requirements, funding, and training.

3.6 Appendices. Appendices may contain additional information used in supporting test program planning.

Appendix A – Test Report Outlines

Table 2. Example of DT&E Report Outline

Section	Section Title	Content
1	Component / Subsystem / System Description	A brief description of the system component to be tested. *Component* is used broadly in this context to include physical, logical, and process elements of the system.
2	Test Objectives	A brief statement of test objectives traceable to requirements.
3	Test and Use Cases	Test and use cases designed to objectively develop information to support test objectives.
4	Test Tools and Resources	A summary of all tools and resources required to execute the tests including identification of test sites.
5	Test Procedure	Reference the appropriate procedures executed, and identify the sequence steps used during the test.
6	Test Constraints/Limitations	Describe any test constraints or limitations (i.e., test platform).
7	Test Results, Schedule, and Success Criteria	A report of all test results, including those not anticipated during the procedure.
8	Test Anomalies	A description of anomalies identified during the test and (if any) workarounds.
9	Recommendations	A list of recommendations based on the test outcomes.
10	Conclusions	A list of conclusions drawn from the test outcomes and success criteria.

Table 3. Example of OT&E Report Outline

Section	**Section Title**	**Content**
1	System Capability Description	A brief description of the system capabilities that will be tested and assessed.
2	Test Objectives	A brief description of test objectives traceable to the requirements.
3	Test Method	A description of the test and data collection method.
4	Test Tools and Resources	A summary of required tools and resources including identification of test sites.
5	Test Constraints/Limitations	Describe any test constraints or limitations (i.e., test platform)
6	Test Results, Schedule, and Success Criteria	A report of all test results, including those not anticipated during the test planning or method.
7	Test Evaluation	An evaluation of the test results.
8	Test Anomalies	A description of anomalies identified during the test and (if any) workarounds.
9	Recommendations	A list of recommendations based on the test outcomes.
10	Conclusions	A list of conclusions drawn from the test outcomes and success criteria.

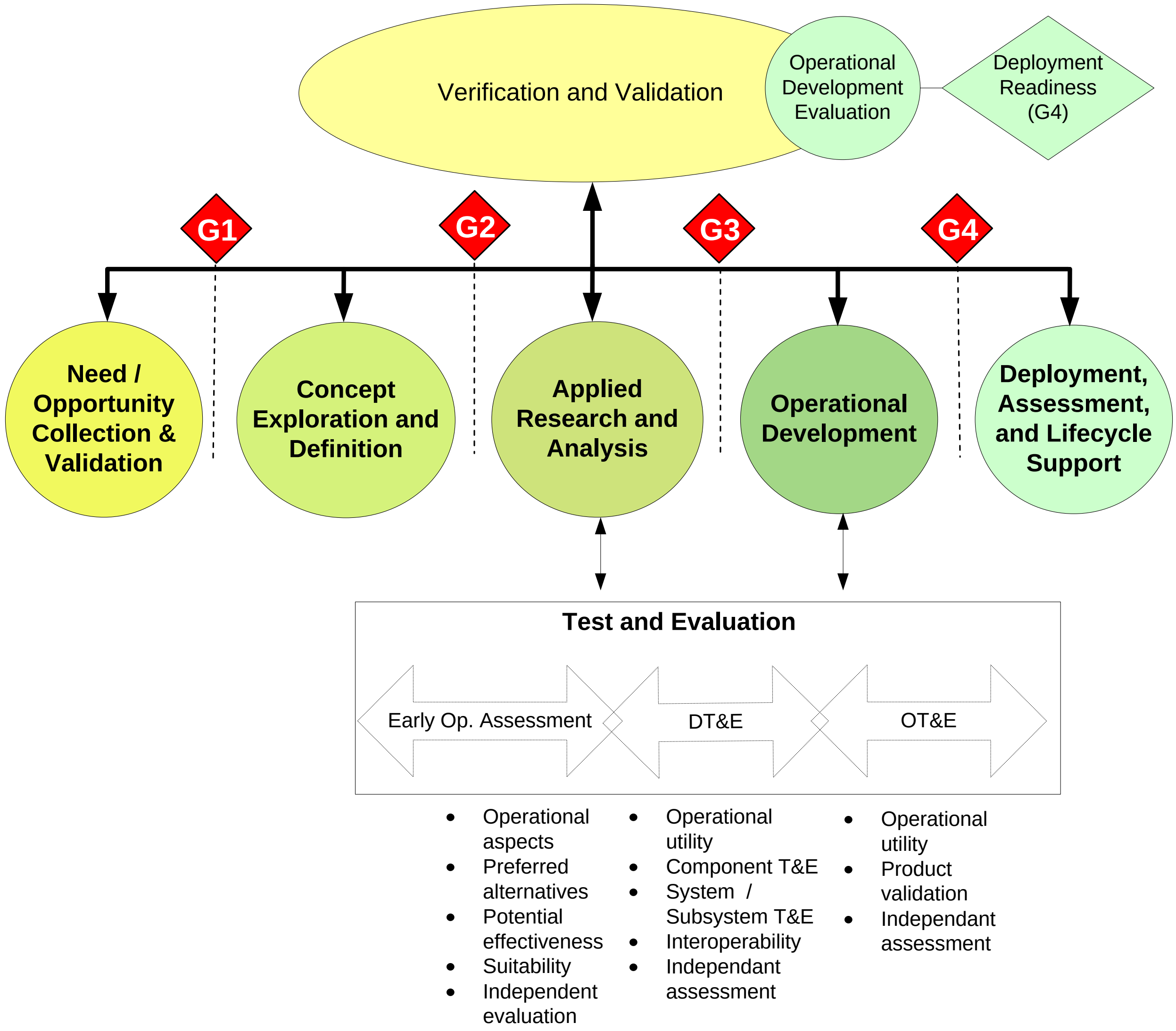

Figure 1. Test and Evaluation Links to the Operations and Services Improvement Process

Appendix B - Definitions

DT&E Development Test & Evaluation verifies that the design solution meets the system technical requirements and the system is prepared for successful Operational Test and Evaluation (OT&E). DT&E activities assess progress toward resolving critical operational issues, validating cost-performance tradeoff decisions, mitigating acquisition technical risk, and achieving system maturity.

OT&E Operational Test & Evaluation programs are structured to determine the operational effectiveness and suitability of a system under realistic conditions, and to determine if the minimum acceptable operational performance requirements as specified in the Concept of Operation / Operational Requirements Document (ConOps/ORD) and reflected by the key performance parameters have been satisfied.

ISSO Information System Security Officer assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.

ST&E Security Test & Evaluation confirms that system security requirements have been appropriately addressed within system design, development, integration and implementation. ST&E activities occur as part of both DT&E and OT&E. ST&E activities may require an independent team to accomplish the activities. ST&E activities must be included in system program plans and budgets.

Test The use of system, subsystem, or component operation to obtain detailed data to verify performance or to provide sufficient information to verify performance through further analysis. Testing is the detailed quantifying method of verification and is ultimately required in order to verify the system design.

Use Case Use cases are detailed, structured, text-based descriptions of interactive usage.

Appendix C - References

1. NWS Policy Directive 10-1, *NWS Requirements, Operations and Services Improvements.*
2. NWS Instruction 10-103, *Operations and Services Improvement Process Implementation.*
3. NWS Policy Directive 80-3, *Systems Engineering*.
4. NWS Instruction 80-303, *Systems Engineering for New Development*.
5. NWS Instruction 80-304, *Software Development*.
6. NWS Policy Directive 60-7*, Information Technology Security Policy*.
7. DOD, Systems Management College, Defense Acquisition University, *Systems Engineering Fundamentals*, 2001.
8. IEEE 1012-1998 *Standard for Software Verification and Validation*, 1998.
9. NWS Instruction 30-301, *System Test (ST) Process*.
10. NWS Instruction 30-302, *Operational Test and Evaluation Process*.
11. NWS Instruction 80-201, *System Commissioning Process*.
12. DOC IT Security Program Policy and Minimum Implementation Standards, Section 6.3.3, *Security Test and Evaluation (ST&E),* Revised June 30, 2005