



**Net-Enabled Command Capability
JOINT TEST AND EVALUATION
DEFICIENCY REPORT
STANDARD OPERATING PROCEDURE
(JT&E DR SOP)**

Version 1.0

29 October 2008

NECC-JT&E-DR-SOP-00206

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

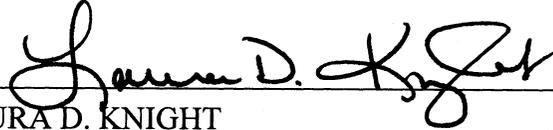
In Collaboration with the USJFCOM and the NECC Component Program Managers for the Navy, Air Force, Army, Marine Corps, and DISA

DISTRIBUTION STATEMENT C: This document is authorized to the U.S. Government agencies and their contractors only to protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means: (June 2007). All other requests for this document will be referred to the Lead OTA, Army Test and Evaluation Command (ATEC) for the NECC Program.

HANDLING AND DESTRUCTION NOTICE: Comply with distribution statement and destroy by any method that will prevent disclosure of contents or reconstruction of the document.

APPROVAL PAGE

Approved by:



Date:

19 Nov 2008

LAURA D. KNIGHT
Joint Program Manager,
Joint Program Management Office (JPMO),
Net-Enabled Command Capability (NECC)

EXECUTIVE SUMMARY

This Joint Test and Evaluation (JT&E) Deficiency Report (DR) Standard Operating Procedure (SOP) outlines the steps required to ensure all software and hardware deficiencies, recommended improvements, and Software Change Requests (SCR) discovered during Net-Enabled Command Capability (NECC) Test, Evaluation, and Piloting (TE&P) activities are handled appropriately, following the intent of joint service deficiency reporting requirements and the NECC Security Classification Guide as well as other classification authoritative documents as applicable. The DR process framework is introduced and specific tasks during each phase are provided. The roles and responsibilities of the various organizations involved in DRs and the relationships among these organizations are defined.

This SOP was drafted in coordination with the Service Operational Test Agencies (OTA), Joint Combat Capability Developer (JCCD), Joint Interoperability Test Command (JITC), Joint Program Management Office (JPMO), and Service Component Program Management Offices (CPMO) membership to the NECC Program's DR Working Group (WG).

Note: The NECC Joint DR WG has not yet selected/recommended a DR data collection tool. It is recognized that such a DR data collection tool must support the entire NECC discrepancy reporting lifecycle. At this time, funding is not available to support the selection and stand-up of a permanent DR database solution. The selection to use the Software Trouble Report (STR) Database, located at SPAWAR Systems Center-San Diego (SSC-SD), California, for FY-09 as the data collection tool has been agreed upon by DR WG as a temporary solution until which time funding supports the acquisition and stand-up of the long-term joint solution. The STR database will also support the identification of hardware discrepancies found during TE&P events. STR database limitations may exist that prevent an automated flow of the DR submission process and any deviations from this SOP will be completed manually and identified in the Detailed Test Plan, if required.

TABLE OF CONTENTS

APPROVAL PAGE	II
EXECUTIVE SUMMARY	III
REVISION HISTORY	IV
1 INTRODUCTION	1
1.1 DOCUMENT PURPOSE	1
1.2 SCOPE.....	1
1.3 APPLICABILITY	1
1.4 TEST TEAM ORGANIZATION	1
2 SERVICE DESK OVERVIEW	2
3 TEST DATA MANAGEMENT	2
3.1 TEST DATA CATEGORIES.....	2
3.2 DEFICIENCY CATEGORIES	4
3.3 TEST DATA LEVELS.....	4
3.4 PRE-DTRG DATA MANAGEMENT	5
3.5 DTRG	6
3.6 POST DTRG ACTIVITIES	7
3.7 CONFLICT RESOLUTION.....	7
3.8 DR RESOLUTION VALIDATION PROCESS	7
4 TEST DATA ACCESS AND RELEASABILITY	8
4.1 TEST ORGANIZATIONS.....	8
4.2 CPMO/JPMO	8
4.3 THE DEVELOPING CONTRACTOR	8
4.4 TEST DIRECTOR/DEPUTY TEST DIRECTORS/SENIOR SERVICE REPRESENTATIVE	9
4.5 SYSTEM USERS AND WARFIGHTERS	9
4.6 RELEASABILITY AND PROHIBITED DISCUSSIONS	9
4.7 DEFICIENCIES REQUIRING TEST TERMINATION	9
5 STR DATABASE	9
5.1 OVERVIEW	9
5.2 SOFTWARE REQUIREMENTS.....	9
5.3 LOCATION/REQUIREMENTS/SUPPORT.....	9
5.4 WEB-BASED DATA ENTRY PROCEDURES	10
APPENDIX A – LIST OF ACRONYMS	11
APPENDIX B – REFERENCES	13
APPENDIX C – DEFICIENCY REPORT PRIORITIES	14
APPENDIX D – TIPR FORM	15

LIST OF FIGURES

Figure 1: Test Data Management Process..... 3
Figure 2: DR Resolution Validation Process 8

LIST OF TABLES

Table 1: Levels of Data from DA PAM 73-1 4

1 INTRODUCTION

1.1 Document Purpose

This Joint Test and Evaluation (T&E) Deficiency Report (DR) Standard Operating Procedure (SOP) provides information and outlines the DR recording and management process established to ensure software and hardware deficiencies and recommendations identified during Net-Enabled Command Capability (NECC) Test Evaluation and Piloting (TE&P) activities are documented and processed in a consistent, efficient and logical manner.

1.2 Scope

This SOP describes the basic procedures and responsibilities for test incident management, from initial documentation of a Test Incident Problem Report (TIPR) through the Daily Test Review Group (DTRG), where TIPRs are validated and promoted to DRs and are made available for data authentication, failure definition scoring and other post-test activities. The processes and procedures provided in this document expand on the concepts and procedures presented in references (a) through (j). Familiarity with these concepts and procedures is essential for all TE&P participants to effectively identify and draft TIPRs and promote them as DRs or a Software Change Request (SCR) within the NECC T&E DR process. This T&E DR SOP leverages Component Program Management Office (CPMO) local help desk procedures and the Joint Technical Operations Control Capability (JTOCC) that provides service desk, configuration management, and service monitoring supporting NECC operations 24/7/365, to include during NECC TE&P activities. The T&E DR processes will supplement, not replace, CPMO local help desk procedures and JTOCC processes as necessary to support T&E data collection requirements.

1.3 Applicability

This procedure applies to all test participants including: Joint Program Management Office (JPMO) and CPMO personnel (to include Net-Ready Key Performance Parameter (NR-KPP) and Information Assurance (IA) personnel), Developmental Test (DT) and Operational Test (OT) personnel, Test Directors (TD), Deputy Test Directors (DTD), senior Service representatives, test participants (users), warfighters, and developing contractors.

1.4 Test Team Organization

References (a), (b), (h), and (j) prescribe roles and responsibilities for T&E planning, conducting, evaluating and reporting NR-KPP, IA, Integrated, DT and/or OT events and the minimum DR requirements. The TD is the CM Test Team (CMTT) DT Lead or CMTT OT Lead and represents the lead DT Agency (DTA) or OT Agency (OTA), as applicable. The supporting DTA/OTA will act in the capacity of DTD and exercise operational control and test management authority over their service test teams. The lead DTA/OTA, in coordination with the supporting DTA/OTA, will include all resource requirements in a consolidated resource estimate. Specific roles and responsibilities for a test will be promulgated in the DT/OT Detailed Test Plan for that specific event. As needed, and at the discretion of the TD/DTD, a senior Service representative may be designated to provide leadership and management of test site activities. Test site leads (including senior Service representatives) and user personnel fall under the operational control of their respective TD/DTD. Data collector (DC) personnel are part of the service test teams and

provide data collection and data entry functions for the TD/DTD. In this document, use of the term “test team member” is the TD/DTD/senior Service representative or appropriate delegated test organization representative. System users or Warfighters are active force/fleet personnel who have been designated to support test operations. “User representative” personnel from the Joint Forces Command and Joint Combat Capability Directorate monitor test event activities and participate in the DTRG.

2 SERVICE DESK OVERVIEW

Per reference (c) and (d), the JTOCC employs a three tier system designed to effectively support incident/problem reporting and resolution.

The NECC-JTOCC is a distributed, net-centric capability that is supported and sustained by participants and users accessing and/or providing operational support from across the Global Information Grid (GIG). Although JTOCC stakeholders are not collocated in a single facility, they cooperatively execute the service management functions. Stakeholders share a common tool suite so that they can effectively collaborate on any issues impacting operations.

The JTOCC is responsible for service provisioning, service management, monitoring, configuration management, and reporting for NECC Capability Modules (CMs). The JTOCC provides a logical management function for NECC NetOps and includes a structured, enterprise-level configuration management process.

JTOCC NetOps support functions include:

- Integration support for CMs migrated to the production environment;
- Service Desk support;
- Monitoring and reporting on NECC applications, systems, services in partnership with local GIG Computing Node personnel, the GIG Infrastructure Service Management Center, and the local Control Communications Center; and
- Configuration management support

3 TEST DATA MANAGEMENT

3.1 Test Data Categories

Any information recorded about the test article or test-related activities during a record test can be considered test data. Test data is not limited to but includes: TIPRs, DRs, SCRs, Observations (OBS), Survey responses, Performance data, and Modeling and Simulation data. Figure 1 identifies the test data management process.

Heavy arrow highlights path of DR for DT/OT events

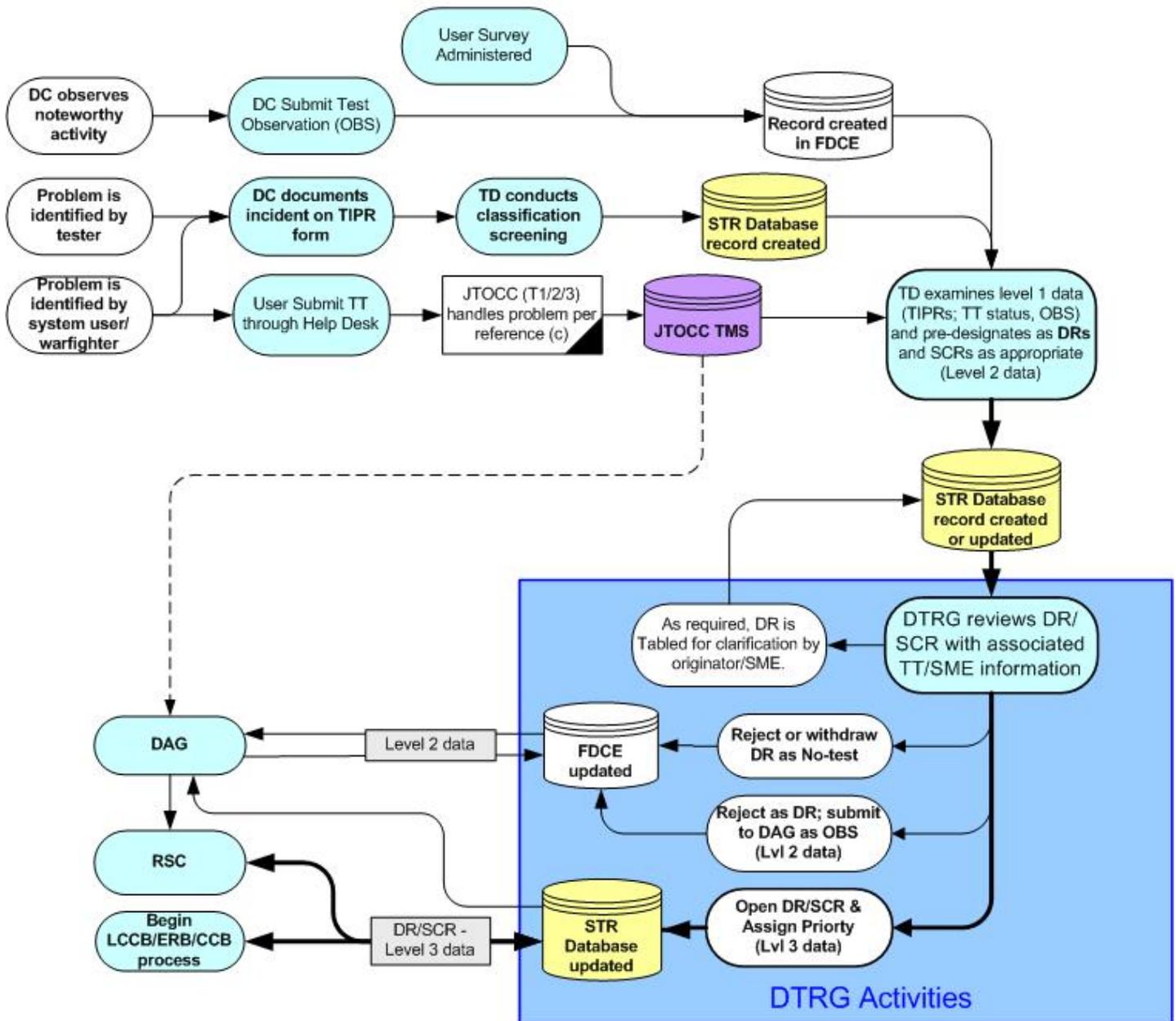


Figure 1: Test Data Management Process

3.2 Deficiency Categories

In order for a DR to be valid, a mission capability must be impacted or a system requirement not met. DRs are assigned a mission impact priority ranging from 1 to 5. Appendix C lists and explains each of the incident priority levels. There are some cases where a potential deficiency is recognized as important to document, but it was either anomalous or cannot be fully characterized within the limitation of the test event. In this case the DR may be “Opened” as a “Watch Item” with no mission impact priority assigned.

If during test, system software changes that do not qualify as DRs and are deemed important or valuable to the test team, an SCR is submitted. SCRs will be examined for completeness and validity (i.e. ensuring the request is not actually a system deficiency) during the DTRG, however; SCRs will not be assigned a mission impact priority by the DTRG.

SCRs may be submitted through the JTOCC trouble desk; however; at the TD/DTD discretion, an SCR may be submitted via the Federated Developmental Certification Environment (FDCE) to the Software Trouble Report (STR) database.

3.3 Test Data Levels

Per reference (e), the level of data to be reviewed by the Data Authentication Group (DAG) may be determined during initial test planning.

The DAG meets while operational tests are being conducted to ensure timely exchange of data among all participating organizations/commands and to build a factual database by assisting in data reduction, data analysis, and investigation of problems surfaced in test data. DAG members will review and authenticate the test conduct, data collection, data reduction, and data set/database contents as indicated by the DAG procedures outlined in the detailed test plan or SOP. The DAG verifies that performance, human factors, and Reliability, Availability, and Maintainability (RAM) data are valid. The DAG procedures may call for examination of data from levels 1–3 in the authentication process. Once the level 3 data set has been reviewed and approved by the DAG, it becomes the authenticated data set, or data set of record for that test. The description of level 1, 2 and 3 data is listed in Table 1 below.

Table 1: Levels of Data from DA PAM 73-1

	Description	Possible forms	Example of Content	Disposition
Level 1 “Raw Data	Data in their original form. Results of field trials just as recorded	Complete data collection sheets, exposed camera film, voice recording tapes, original instrumentation magnetic tape or printouts, original videotapes, completed questionnaires, and/or interview notes.	<ol style="list-style-type: none"> 1. All reported target presentations and detection. 2. Clock times of all events. 3. Azimuth and vertical angle from each flash base for each flash. 4. Recording tapes of interviews. 	Accumulated during trials for processing. Usually discarded after use. Not published.

	Description	Possible forms	Example of Content	Disposition
Level 2 "Reduced Data"	Data taken from the raw form and consolidated. Invalid or unnecessary data points deleted. Trials declared "No Test" deleted.	Confirmed and corrected data collection sheets, film with extraneous footage deleted, corrected tapes or printouts, and original raw data with "No Test" events marked out.	<ol style="list-style-type: none"> 1. Record of all valid detections. 2. Start and stop times of all applicable events. 3. Computed impact points of each round flashed. 4. Confirmed interview records. 	Produced during processing. Usually discarded after use. Not published.
Level 3 "Ordered Data"	Data that have been checked for accuracy and arranged in convenient order for handling. Operations limited to counting and elementary arithmetic	Spread sheet, tables, typed lists, ordered and labeled printouts, purified and ordered tape, edited film, and/or edited magnetic tapes.	<ol style="list-style-type: none"> 1. Counts of detections arranged in sets showing conditions under which detections occurred. 2. Elapsed times by type of event. 3. Impact points of rounds by condition under which fired. 4. Interview comments categorized by type. 	Not usually published but made available to analysts. Usually stored in institutional databanks. All or part may be published as supplements to the test report.

3.4 Pre-DTRG Data Management

Every TIPR will be screened by the originator with the deliberate purpose of verifying its security classification prior to entry into the STR database.

Prior to the DTRG, all unclassified TIPRs and SCRs are recorded by the originator or data collector and maintained in the STR database which resides on the Non-Secure Internet Protocol Routing Network. A DC or other test team member will record information surrounding a test incident or potential test incident in a TIPR or Observation (OBS) form, depending on guidance provided by the TD/DTD. A TIPR may be initiated anytime during a test event and initiating a TIPR does not necessitate a call or request to the JTOCC service desk. A Trouble Ticket (TT) entered in Trouble Management System (TMS) through user-help desk interaction is processed as described in section 2.

Classified TIPRs and SCRs are recorded and maintained on Defense Knowledge Online-Secure (DKO-S).

Throughout the test period appropriate test team personnel (TD, DTD, senior Service representative, or other designated individual) will obtain a detailed status of test related TTs

including their current elevated status (i.e. Tier 2, 3) and will compare this data with other data collected by the test team. Depending on the nature and/or state of a TT, test team members will draft or complete initiated TIPRs and SCRs, and will promote or publish them to the STR database as “Candidate DRs” for the next DTRG. It is the responsibility of the TD/DTD to ensure that candidate DRs and SCRs are as accurate and complete as possible. Appendix D provides an example of the TIPR form. DRs will include the following data fields at a minimum:

- Title
- Test site location and date
- Site test director, TIPR/SCR originator, screener and SME
- Mission Capability Package, Capability Module, Capability Package and Spiral
- Problem source (Software, documentation, etc.) and problem type (TIPR or SCR)
- System down time, repeatability of problem
- Sequence of events and detailed problem description
- User assigned priority, mission impact and work around (if any)
- Test measure the issue affects or is associated with
- Security classification

3.5 DTRG

The DTRG is the forum by which all TIPRs are reviewed and approved as DRs within the NECC program. The DTRG will always be chaired by the test director or appropriate delegated individual. The TD will designate an individual with appropriate role permissions to update DRs within the STR database during the DTRG.

DTRG participants include the TD, DTD, senior Service Representatives, CPMO personnel, JPMO personnel, Warfighter Representatives, CM developer personnel, SMEs, data collectors, and any other personnel, as required, to conduct a thorough review of DRs and SCRs.

The DTRG will normally convene daily during test events as test conditions permit. Regardless of whether or not a DTRG is held, the program offices will be notified within 24 hours of any potential priority 1 deficiencies discovered during test. Safety-related Priority 1 TIPRs will be forwarded immediately to the TD or DTD; Priority 2 DRs, within 3-workdays.

During the DTRG, candidate DRs are reviewed thoroughly and updated with additional details, provided by other test team or SME personnel as appropriate. Once the DTRG determines that the DR is accurate and complete, it is placed into “Open” status. If the DTRG determines the priority assigned is incorrect based on additional information provided, they may change it, but the originators priority will always remain as part of the DR history. If additional research is determined necessary, the TIPR will be put into a “Tabled” status. Once research is complete and the TIPR has been updated, it is resubmitted to the DTRG for review. The DTRG may determine that a DR is not appropriate; in which case, it will be “Rejected”. A Rejected DR will remain in the STR database, and either will be scored “Non-test” or will be converted to an OBS.

The recommended order of reviewing DRs is candidates for Priority 1 DR, all resubmitted DRs, remaining DRs, and then all SCRs. To facilitate expedient resolution, a Priority 1 DR may require an initial submission with a minimum of information followed up by further information as it becomes available.

Once DRs and SCRs are “Opened” by the DTRG, they are available to the RAM Scoring Conference (RSC), reference (e) and the CCB, reference (f), for their respective actions.

3.6 Post DTRG Activities

Per reference (e) and (k), the RSC will convene after the DTRG and review all opened DRs to determine and score operational mission failures (OMF) and non-essential function failures (NEFF). The primary source of information for the RSC is DRs. If a DR is scored as an OMF or NEFF, this information will be recorded in the STR database by test team member with appropriate write access.

3.7 Conflict Resolution

Per reference (a), if there is disagreement about a DR (i.e. the TD or DTD does not concur with a DR as written) they may attach their non-concurrence rationale to the DR.

3.8 DR Resolution Validation Process

Upon corrective action to resolve the DR, the CPMO/JPMO will update the STR database with the corrective action and nominate the DR for resolution validation. The Test Planning Team (TPT) and CMTT will review and determine the appropriate test event to validate the fix action. Once the DR has been confirmed as fixed, the STR database will be updated to close the DR. (See Figure 2)

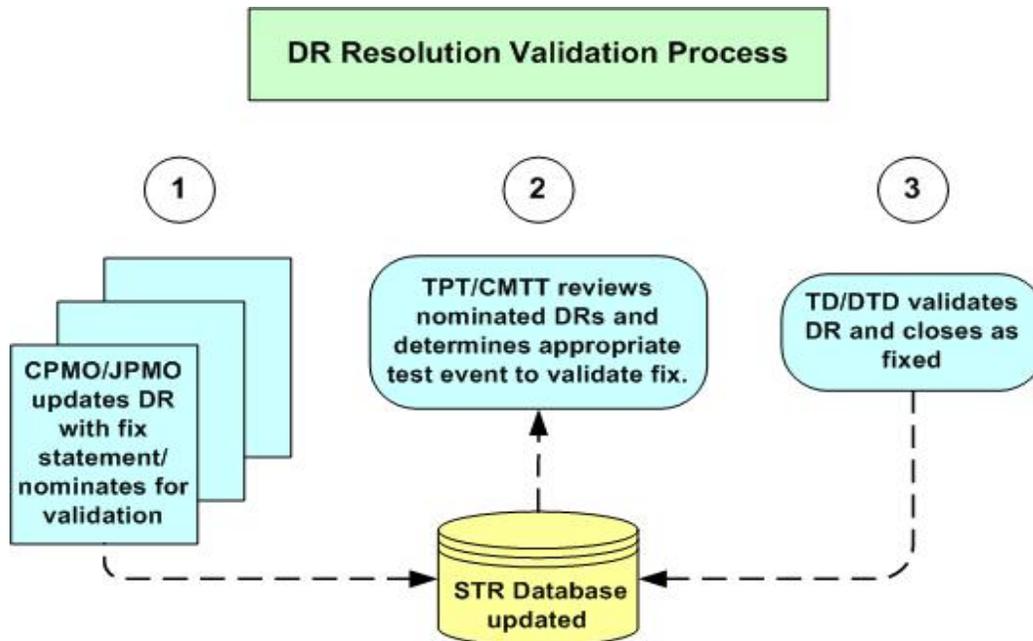


Figure 2: DR Resolution Validation Process

4 TEST DATA ACCESS AND RELEASABILITY

4.1 Test Organizations

The STR database maintains an audit trail of all updates made to a DR/SCR. Data will be shared among the test team through the use of the JTOCC TMS, JDCAT, FDCE, and STR database. Per reference (a), release of data outside of the test team, except as described below, will require the approval of the TD/DTD.

4.2 CPMO/JPMO

The CPMO/JPMO will have access to candidate DRs within the STR database while in the pre-DTRG status in order to provide technical comments to the TIPRs. Additionally, the CPMO/JPMO will have access to “Opened” DRs and SCRs to facilitate Local Configuration Control Board (LCCB)/ERB/CCB and other board requirements.

4.3 The Developing Contractor

The developing contractor will have access to the STR database as requested by the CPMO/JPMO. The developing contractor will be able to provide technical comments in the developer comments area only. The developing contractor may be present for discussions involving DRs per DoD 5000.2. Inputs by the contractor will be limited to the technical aspects of the reports for the purpose of helping fully assess the deficiency and to provide TIER 1/2/3 Service Desk technical support clarification as outlined in the Concept of Operations for NECC JTOCC Network Operations. Under no circumstances will the contractor influence the assigning of priority to DRs In Accordance With Title 10, Section 2399 and DoD 5000.2R.

4.4 Test Director/Deputy Test Directors/Senior Service Representative

The TD/DTD/senior Service representative has full access to TIPRs, DRs, and SCRs and full search and view access to the TMS, Survey Tool, FDCE, and STR database. The TD or appropriately delegated personnel will have role-based permission to a) assign TIPRs to DR status to facilitate the DTRG and b) edit privileges to current test TIPRs within the STR database. Appropriate personnel as designated by the lead service OTA will have write access to the STR database for the specific purpose of updating DRs with Failure Definition Scoring Criteria (FDSC) results.

4.5 System Users and Warfighters

System users and warfighters can create new TIPRs/SCRs within the STR database however, only read access is granted once a TIPR/SCR has been submitted.

4.6 Releasability and Prohibited Discussions

Per reference (a), release of data outside of the test team, except as described below, will require the approval of the TD/DTD. Test team members (test participants and testers) are prohibited from discussing potential deficiencies, draft deficiencies, and watch items outside of the test team, until after they are approved by the DTRG or without the expressed approval of the TD/DTD. The pre-approved exception to this rule is the use of the Tier 1/2/3 Service Desk process as operationally representative and as described in this procedure. In this case, discussions will be limited to the technical aspects of the deficiency/incident.

4.7 Deficiencies Requiring Test Termination

In the event that a deficiency warrants suspension/termination of the test, the circumstances should be reported immediately to the TD who will determine if the test should be suspended or terminated until the deficiency is corrected. All testing will be suspended to afford participating Services an opportunity to discuss the deficiency. If appropriate, the TD may determine that tests can continue safely on a limited basis pending subsequent correction of the deficiency.

5 STR DATABASE

5.1 Overview

All TIPR/SCRs will be entered into the STR database after appropriate screening is performed as previously described. STR database is a web based data collection tool used to support test events through structured collection, analysis and processing of deficiencies generated by test participants.

5.2 Software Requirements

Web browser – Internet Explorer (version 6.0 and above) or Firefox (version 2.0 and above).

5.3 Location/Requirements/Support

- a. Website Address: <https://navycpmo.spawar.navy.mil>
- b. Security and Access Information: Common Access Card or Software Public Key Infrastructure is required for access. Account registration can be completed online at

the following location:

<https://navycpmo.spawar.navy.mil/Registration/Registration.cfm>

- c. Technical Support: For technical support such as account questions or technical issues accessing the database, please send an email to: neccdrtech@spawar.navy.mil.

5.4 Web-based data entry procedures

Test participants will be instructed in the proper use of the STR database prior to commencement of test operations. These procedures are also located online at the above web site address.

APPENDIX A – LIST OF ACRONYMS

Acronym	Definition
C2	Command and Control
CCB	Configuration Control Board
CM	Capability Module
CMTT	Capability Module Test Team
CPMO	Component Program Management Office
DAG	Data Authentication Group
DC	Data Collector
DISA	Defense Information Systems Agency
DKO-S	Defense Knowledge Online-Secure
DoD	Department of Defense
DR	Deficiency Report
DT	Developmental Test
DTA	Developmental Test Agency
DTD	Deputy Test Director
DTRG	Daily Test Review Group
ERB	Engineering Review Board
FDCE	Federated Developmental Certification Environment
FDSC	Failure Definition Scoring Criteria
GIG	Global Information Grid
JPMO	Joint Program Management Office
JTOCC	Joint Technical Operations Control Capability
LCCB	Local Configuration Control Board
NECC	Net-Enabled Command Capability
NEFF	Non-Essential Function Failure
OBS	Observations
OMF	Operational Mission Failure
OT	Operational Test
OTA	Operational Test Agency
POC	Point of Contact
RAM	Reliability, Availability, and Maintainability
RSC	RAM Scoring Conference

Acronym	Definition
SCR	Software Change Request
SME	Subject Matter Expert
SOP	Standard Operating Procedure
STR	Software Trouble Report
TD	Test Director
T&E	Test and Evaluation
TE&P	Test Evaluation and Piloting
TIPR	Test Incident Problem Report
TMS	Trouble Management System
TPT	Test Planning Team
TT	Trouble Ticket

APPENDIX B – REFERENCES

- a. NECC Memorandum of Agreement on Multi-Service Operational Test and Evaluation (MOT&E) and Operational Suitability Terminology and Definitions, Oct 2007
- b. NECC Joint Systems Team (JST) Test and Evaluation Charter, Ver. 1.5, xx Oct 2008
- c. Concept of Operations (CONOPS) for NECC Joint Technical Operations Control Capability (JTOCC), Ver. 1.6.2, 16 May 2008
- d. NECC Joint Technical Operations Control Capability (JTOCC) Execution Plan, Ver. 0.6, 22 February 2008
- e. Department of the Army Pamphlet 73-1, Test and Evaluation in Support of Acquisition, 30 May, 2003
- f. NECC Increment 1 System Development and Demonstration (SDD) Phase Configuration Management Plan, Ver. 1.0, 27 July 2007
- g. NECC Systems Engineering Plan Increment 1 Milestone B, Ver. 1.0, 9 August 2007
- h. NECC Increment 1 Capstone Test and Evaluation Master Plan (TEMP), Ver. 1.0, 6 August 2007
- i. NECC Security Classification Guide, Ver. 0.0.3, 14 September 2008
- j. NECC Capability Provisioning Event (CPE) Standard Operating Procedure (SOP), Ver. 2.0, 22 October 2008
- k. NECC Failure Definition Scoring Criteria (FDSC), First Draft, 17 October 2008

APPENDIX C – DEFICIENCY REPORT PRIORITIES

Priority		Applies if a problem could:
1	a	Prevent the accomplishment of an operational or mission essential capability.
	b	Jeopardize safety, security, or other requirement designated "critical".
2	a	Adversely affect the accomplishment of an operational or mission essential capability and no work-around solution is known.
	b	Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known.
3	a	Adversely affect the accomplishment of an operational or mission essential capability but a work-around solution is known.
	b	Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known.
4	a	Result in a user/operator inconvenience or annoyance but does not affect required operational or mission essential capability.
	b	Result in inconvenience or annoyance for development or support personnel, but does not prevent the accomplishment of those responsibilities.
5		Any other effect.

APPENDIX D – TIPR FORM

NECC TEST INCIDENT / PROBLEM REPORT (TIPR) FORM

TIPR Title		
Location	Site Test Director	Originator
Screener	Subject Matter Expert	Date Problem Found
Mission Capability Package	Capability Module Name	Capability Package
Capability Module Spiral	Problem Source	Repeatable
	SW / HW / Documentation / Other	YES NO
System Downtime (if any)	Problem Type	User Priority
	DR SCR	1 2 3 4 5
Sequence of Events		
Problem Description		
Workaround		
Mission Impact (Major, Moderate, Minor – Justify)		
MOE / MOP / MOS		
Security Classification	Classification Official (print, sign, date)	
UNCLASSIFIED / SECRET		
NECC TIPR Tracking No:		