Defense Information Systems Agency

A Combat Support Agency

JITC Standards Research (JSR) Team

J-RAD 101

Strategic Planning and Engineering Division

April 2012

DISA
A Combat Support Agency

Agenda

- Who: JSR Team
- Why: Interoperability/Standards Requirements
- How: Risk Assessments
- What: JSR Services Available
- Tools: J-RAD Web Interface ← NEW!

DISA
A Combat Support Agency

JITC Standards Research (JSR) Team

- JITC Standards Risk Assessment Methodology
  - NR-KPP Guidebook, Appendix E (NR-KPP_Helpdesk@disa.mil)
- J-RAD population and maintenance
  - Standards research
- JITC Standards Research (JSR) Services Available
  - Full Service
  - Self Service

DISA
A Combat Support Agency

Interoperability Requirement

- **GIG Technical Profiles (GTP)**

Table B-5. DISR Compliance

System: Name — StdV-1 (TV-1) last updated on: DD MMM YYYY

Service Area	Standard Identifier	Title Of Standard	DISR Status	Risk/ Rationale	Evaluation Method	Status

NOTES:

1.
2.

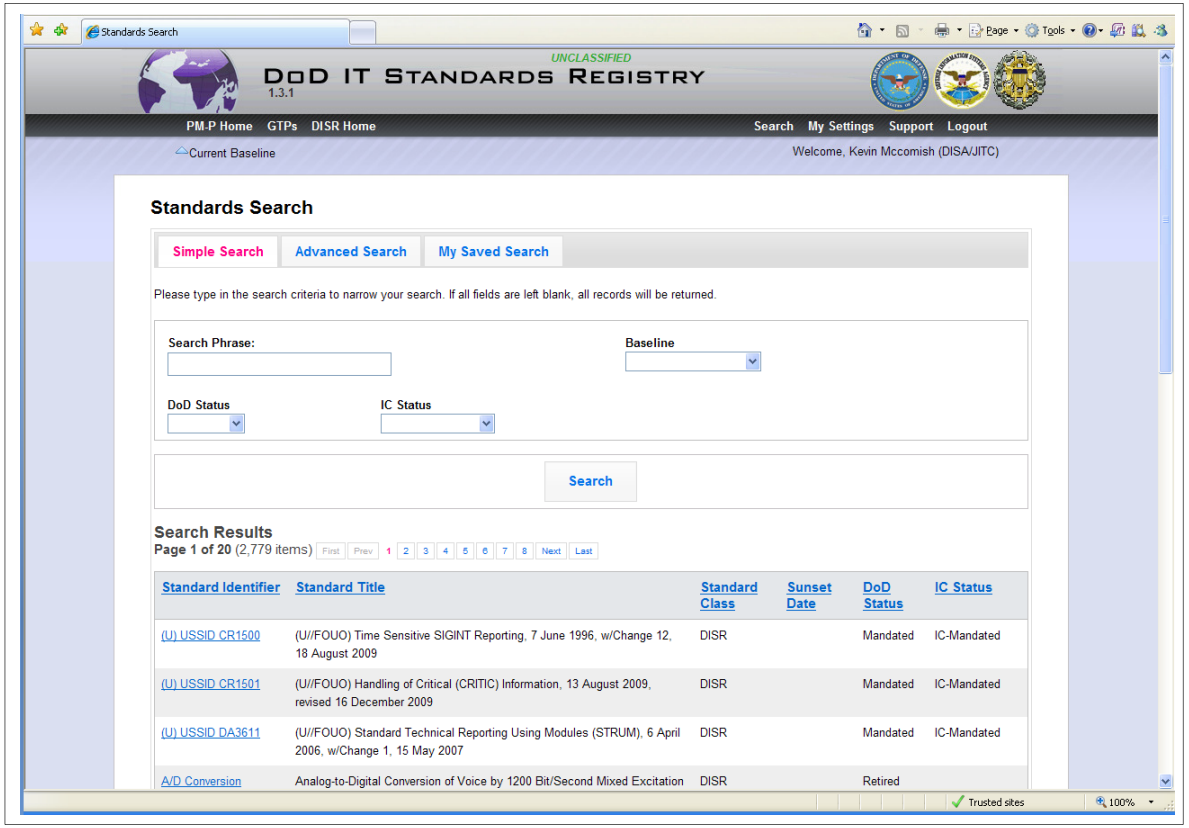
LEGEND:

DISR	DoD Information Technology Standards Registry	TV-1	Technical View Standards Profile
StdV-1	Standard View Profile		

DISA
A Combat Support Agency

DISR Online

- **DoD IT Standards Registry (DISR)**
  - **New website**: https://gtg.csd.disa.mil/disr/dashboard.html



DISA

A Combat Support Agency

TV-1 Example

Technical Standards View (TV-1)

Standards Profile for AUTOMATIC IDENTIFICATION SYSTEM

DISR System Profile:	TV-1 for Navy Automatic Identification System
System Description:	This TV-1 standards profile is for AIS Increment 1 on U.S. Navy shore, surface, and subsurface platforms.
System Classification:	Unclassified
Created by:	Scott Thompson
Published Date:	2009-09-23
CDD or ISP Stage 1:	yes

Technical Standards View (TV-1) - The Technical Standards Profile collects the various systems standards rules that implement and sometimes constrain the choices that can be made in the design and implementation of an architecture.

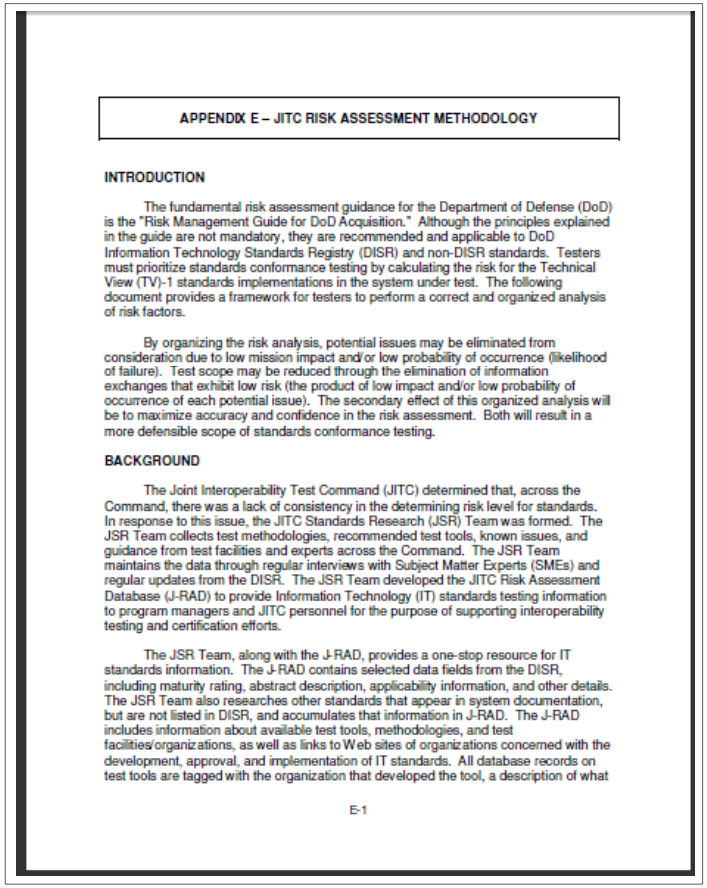
IT Profile:	Navy AIS
IT Description:	This TV-1 profile includes the probable and possible standards applicable to AIS on Navy ships and platforms.
IT Profile Classification:	Unclassified
Last Updated:	2009-09-23

Service Area	Standard Identifier	Title of Standard	Published Status	Sunset	Current Status	Sunset
Military Messaging	ANSI/IEEE 754	Binary Floating-Point Arithmetic, March 21, 1985	Mandated		Mandated	
Document Interchange	CISS GJXDM	Global Justice XML Data Model, Version 3.0.3	Mandated		Mandated	
Document Interchange	CISS ISM: XML	Common Information Sharing Standard for Information Security Marking: XML Implementation, Implementation Guide, Release 2.0.3, 15 February 2006	Mandated		Mandated	
Authentication	CMS/XML Digital Signature Profiles v1.1	DoD Digital Signature Implementation Profiles	Mandated		Mandated	
Application-Oriented (GPS)	ICD-GPS-227	Navstar GPS Selective Availability and Anti-Spoofing (SA/A-S) Host Application Equipment (HAE) Design Requirements with the Selective Availability Anti-Spoofing Module (SAASM), 26 November 2003	Mandated		Mandated	
C4ISR: Payload Platform	IEEE 1394	High Performance Serial Bus, December 1995	Mandated		Mandated	
C4ISR: Payload Platform	IEEE 1394a	High Performance Serial Bus, Attachment 1, 2000	Mandated		Mandated	
Network Technologies	IEEE 802.1X:2004	Local and Metropolitan Area Networks - Port Based Network Access Control	Mandated		Mandated	
Network Technologies	IEEE 802.3-2005	Local and Metropolitan Area Networks - Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision	Mandated		Mandated	

DISA
A Combat Support Agency

JITC Standards Risk Assessment Methodology

- **Follows DoD Risk Methodology**
- **Accurate Risk Calculation**
- **Promotes development of supporting rationale (for defensible test plans)**



APPENDIX E – JITC RISK ASSESSMENT METHODOLOGY

INTRODUCTION

The fundamental risk assessment guidance for the Department of Defense (DoD) is the "Risk Management Guide for DoD Acquisition." Although the principles explained in the guide are not mandatory, they are recommended and applicable to DoD Information Technology Standards Registry (DISR) and non-DISR standards. Testers must prioritize standards conformance testing by calculating the risk for the Technical View (TV)-1 standards implementations in the system under test. The following document provides a framework for testers to perform a correct and organized analysis of risk factors.

By organizing the risk analysis, potential issues may be eliminated from consideration due to low mission impact and/or low probability of occurrence (likelihood of failure). Test scope may be reduced through the elimination of information exchanges that exhibit low risk (the product of low impact and/or low probability of occurrence of each potential issue). The secondary effect of this organized analysis will be to maximize accuracy and confidence in the risk assessment. Both will result in a more defensible scope of standards conformance testing.

BACKGROUND

The Joint Interoperability Test Command (JITC) determined that, across the Command, there was a lack of consistency in the determining risk level for standards. In response to this issue, the JITC Standards Research (JSR) Team was formed. The JSR Team collects test methodologies, recommended test tools, known issues, and guidance from test facilities and experts across the Command. The JSR Team maintains the data through regular interviews with Subject Matter Experts (SMEs) and regular updates from the DISR. The JSR Team developed the JITC Risk Assessment Database (J-RAD) to provide Information Technology (IT) standards testing information to program managers and JITC personnel for the purpose of supporting interoperability testing and certification efforts.

The JSR Team, along with the J-RAD, provides a one-stop resource for IT standards information. The J-RAD contains selected data fields from the DISR, including maturity rating, abstract description, applicability information, and other details. The JSR Team also researches other standards that appear in system documentation, but are not listed in DISR, and accumulates that information in J-RAD. The J-RAD includes information about available test tools, methodologies, and test facilities/organizations, as well as links to Web sites of organizations concerned with the development, approval, and implementation of IT standards. All database records on test tools are tagged with the organization that developed the tool, a description of what

E-1

http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf

DISA
A Combat Support Agency

Assessing Risk

- **Risk = Operational Impact x Likelihood**
- **Operational Impact**
  - **Implementation of standard**
- **Likelihood**
  - **Maturity of standard**
  - **Maturity of system**

DISA
A Combat Support Agency

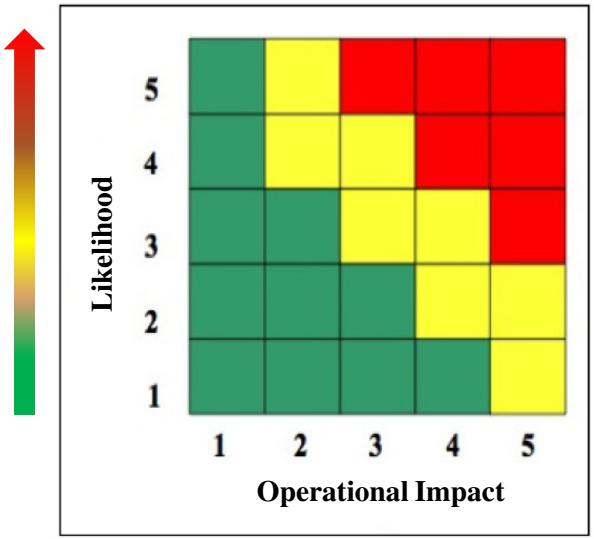
Risk Assessment: Likelihood of Failure

- **Based on:**
  - Known Issues
  - History of the standard
  - Maturity/Development Status
  - How the standard is implemented
  - Maturity of Implementation
- **Resources**
  - DISROnline
  - World Wide Web
  - Subject Matter Experts
  - Communities of Practice/Interest
  - Standard Development Organizations (SDOs)

DISA
A Combat Support Agency

Determining Likelihood of Failure

HIGH = Standard is highly likely to be implemented incorrectly.



LOW = Standard is probably implemented correctly.

DISA
A Combat Support Agency

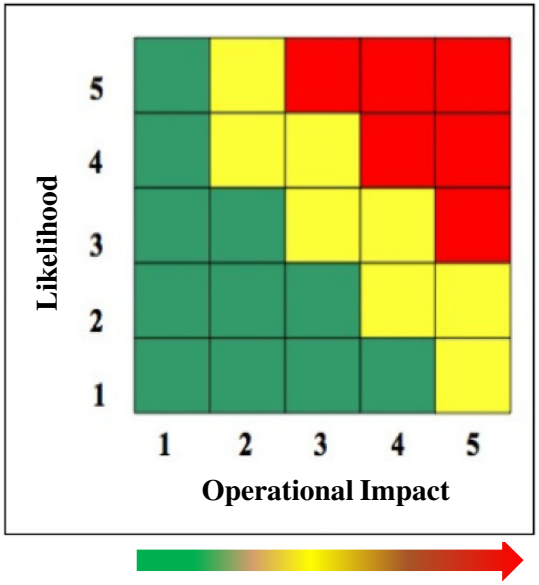
Risk Assessment: Operational Impact

- **Based on:**
  - How the standard is implemented
  - What information exchange(s) the standard supports
  - Criticality of the information exchange or node
- **Resources:**
  - System Architecture Products
  - Integrated Architecture Traceability Matrix (IATM)
  - Traceability between joint critical information exchanges and implementation of a standard
  - Tester input!!!

DISA
A Combat Support Agency

Determining Operational Impact

HIGH = Proper implementation of the standard is required for interoperability of a joint critical operational interface or information exchange.



LOW = Standard implementation does not impact interoperability or the mission.

DISA
A Combat Support Agency

Risk Estimation System 1

	Operational Impact	Likelihood	Risk
HTML 4.01	HIGH Used in JCOA*. Priority users would be unable to view data.	LOW Well-established. Mature standard.	HIGH
DDMS	LOW Not used in JCOA.*	MEDIUM Occasional implementation errors.	LOW

*JCOA – Joint Critical Operational Activity

DISA
A Combat Support Agency

Risk Estimation System 2

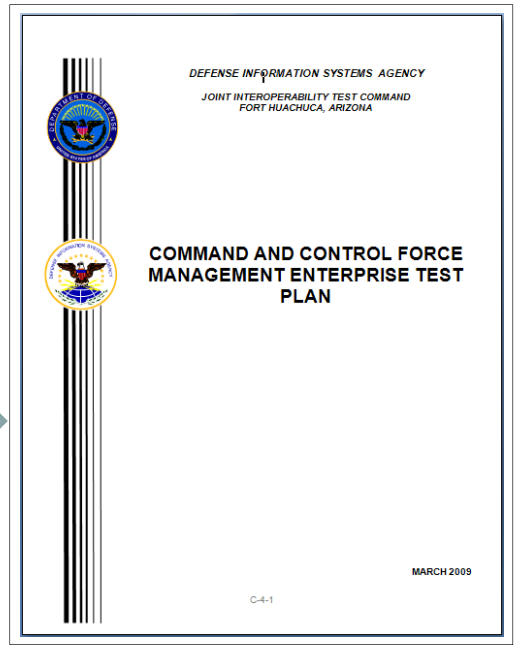
	Operational Impact	Likelihood	Risk
HTML 4.01	NONE Not used in JCOA.	LOW Well-established. Mature standard.	LOW
DDMS	HIGH Used in JCOA. Priority users would be unable to locate data.	HIGH Occasional implementation errors. Newly adopted and untested data schema.	HIGH

DISA
A Combat Support Agency

Prioritize Testing

- **Risk Assessment**
- **Test Planning**

	Operational Impact	Likelihood	Risk
HTML 4.01	NONE Not used in JCOA.	LOW Well-established. Mature standard.	LOW
DDMS	HIGH Used in JCOA. Priority users would be unable to locate data.	HIGH Occasional implementation errors. Newly adopted and untested data schema.	HIGH


DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

COMMAND AND CONTROL FORCE MANAGEMENT ENTERPRISE TEST PLAN

MARCH 2009

C-4-1

DISA
A Combat Support Agency

JSR Team: Full Service Risk Assessment

Risk Assessment Worksheet

	A	B	C	G	H	I	J
1	TV-1 Header	Service Area	Standard ID	Known Issues	Test Tools and Advice	Summary of Standard	Supporting Rationale for Likelihood (from JSR Team)
2		Electronic Data Interchange (EDI)	ANSI ASC X12	NIST proposed withdrawing FIPS PUB 161-2 from subscriiption support as outdated, in 2008. (Fed Register, 2 SEP 2008, Pg 51276)	Use XMLSpy to verify schema validity.	EDI is the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient.	FIPS PUB 161-2 is mature, latest draft 4 submitted in 1997. DoD has 6 working groups supporting the NIST ASC. ASC has representatives from over 300 companies.
3		C4ISR Payload Platform	ANSI X3.230:1999	This is a fee-based standard ($30 on ANSI site)	No test methodology provided.	Fibre Channel is an efficient, high-speed, serial data communication technology for use in many environments including near-real-time high-speed data transfer, and local/campus networking environments. The Fibre Channel Physical and Signaling standards pertain to the first three layers of the Fibre Channel stack (FC0, FC1, and FC2). FC0 addresses the physical media, FC1 discusses the data-encoding scheme, and FC2 addresses the framing protocol and flow control.	The standard original publication date is 1994. The standard is also ISO 14165-141. It is cited in numerous commercial products.
		Product Data Interchange	ANSI/AIM-BC1		No test methodology provided.	This standard is a description of the two-dimensional bar code symbology, Code 39, used to identify packages and products including symbol structure, start and stop characters, quiet zones, and check character. It includes necessary additional pass-fail parameters for the symbology required	Numerous vendors provide products for the encoding, printing, and reading of Code 39 barcodes. The standard was adopted by DoD in June 1997 to replace MIL-STD-1189B.

Risk Assessment Report

Full-Service Standards Report

Navy Enterprise Resource Planning

17 February 2012

JITC STANDARDS RESEARCH TEAM

The Joint Interoperability Test Command (JITC) Risk Assessment Database (J-RAD) provides IT standards testing information to program managers and JITC personnel for the purpose of supporting interoperability testing and certification efforts.

The JITC Standards Research (JSR) Team collects test methodologies, recommended test tools, known issues, and guidance from test facilities and experts across the Command. The JSR Team maintains the data through regular interviews with Subject Matter Experts (SMEs) and regular updates from the Department of Defense (DoD) Information Technology Standards Registry (DISR).

The JSR Team performs unclassified research on required standards and uses the JITC Risk Assessment Methodology to prepare risk assessment reports for full-service customers. The JITC Risk Assessment Methodology is based on the "Risk Management Guide for DoD Acquisition" and is summarized in the following document.

JITC RISK ASSESSMENT REPORT

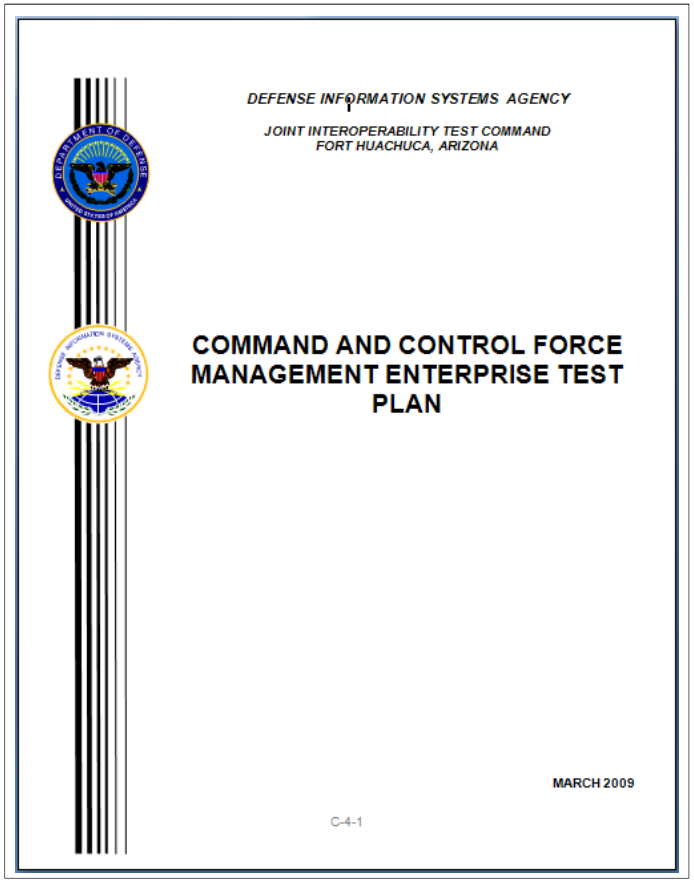
The JSR Team used the J-RAD and other standards research to produce this Initial Risk Assessment. The report represents the modified methodology the team will be applying. The accompanying worksheet, with supporting rationale, calculates risk based on the estimation of Likelihood and Impact risk factors. The ratings range from a low of "1" to a high of "5" for both factors.

The JSR Team has entered an initial Likelihood value in the worksheet. The test

DISA
A Combat Support Agency

JSR Team: Full Service Risk Benefits

- Estimate level of risk
- Prioritize testing
- Justification for priority of testing
- Rationale to support testing decisions
- Plan for test resources


DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

COMMAND AND CONTROL FORCE MANAGEMENT ENTERPRISE TEST PLAN

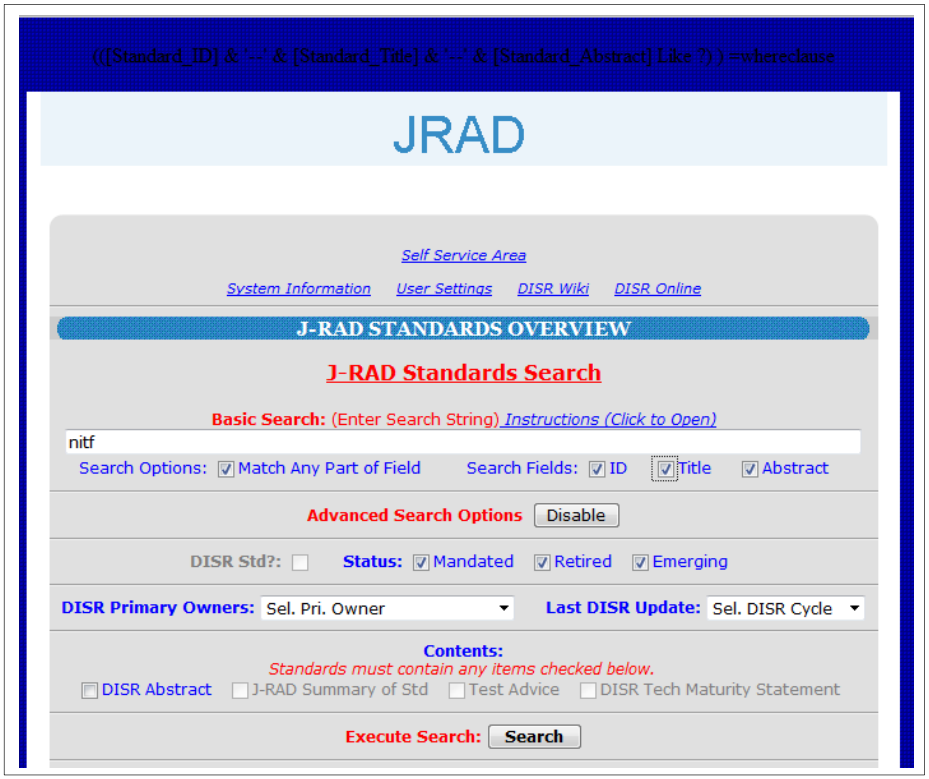
MARCH 2009

C-4-1

DISA
A Combat Support Agency

What is J-RAD?

- **Unclassified MS Access Database**
- **Standards Conformance Test Planning Tool for JITC**
- **Repository for IT standards testing information**



DISA
A Combat Support Agency

JSR Team: J-RAD Self-Service

- **Current J-RAD (located on T: drive)**
  - **Instructions for access: http://jitc.fhu.disa.mil/cgi/jsr/downloads/jsr_request.pdf**
- **New web-enabled J-RAD Self Service**
  - **Coming Soon!**

DISA
A Combat Support Agency

Helpful Links

- **JSR Page on JITC website**
  - http://jitc.fhu.disa.mil/cgi/jsr/
- **JSR Methodology**
  - http://jitc.fhu.disa.mil/cgi/jsr/downloads/nrkpp_guidebook_appdxe.pdf
- **Submit a JSR Request**
  - http://jitc.fhu.disa.mil/cgi/jsr/#
- **NR-KPP Guidebook**
  - https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=347416


DEFENSE INFORMATION SYSTEMS AGENCY