NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

Test Plan Framework for Cross Domain Solution (CDS) Devices

By: **Peter R. Byrd**

June 2010

Advisors: **Brad Naegle**
Michael Boudreau

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project	
4. TITLE AND SUBTITLE Test Plan Framework for Cross Domain Solution (CDS) Devices			**5. FUNDING NUMBERS**
6. AUTHOR(S) Peter R. Byrd			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number_____			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

DoD envisions and is currently developing a wide array of System of Systems and Net-centric warfighting systems that interconnect with many platforms and information repositories designed to provide warfighters information superiority over any adversary. It is critical that information and data passing through and between these systems is secure against any threat or attempt to access, manipulate, or change the data in any way. In addition, these systems are beginning to interconnect with other federal systems outside the purview of DoD.

The DoD and other federal entities have developed differing certification processes and differing test and evaluation requirements to support the certification process. As the need for cross domain interconnectivity increases, the need for more standardized certification test and evaluation processes becomes apparent.

The Joint Applied Project investigates and provides a comprehensive overview of the current Certification Test and Evaluation (CT&E) testing and reporting practices within the National Security Agency. The goal of this project is to identify and document both the process and methodology currently in use during CT&E testing, and to analyze alternative methods to enhance the efficiency and reduce the test duration using a Test Plan Framework.

14. SUBJECT TERMS CDS, CT&E, NSA, NIST, RDAC			**15. NUMBER OF PAGES** 49
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified/FOUO	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

TEST PLAN FRAMEWORK FOR CROSS DOMAIN SOLUTION (CDS) DEVICES

Peter R. Byrd, Department of the Army
B.S., Computer and Information Science, University of Phoenix Online, 2006

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Author: _____
Peter R. Byrd

Approved by: _____
Brad Naegle, Lead Advisor

_____
Michael W. Boudreau, Associate Advisor

_____
William R. Gates, Ph.D., Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

TEST PLAN FRAMEWORK FOR CROSS DOMAIN SOLUTION (CDS) DEVICES

ABSTRACT

Department of Defense envisions, and is currently developing, a wide array of System of Systems and Net-centric warfighting systems that interconnect with many platforms and information repositories designed to provide warfighters information superiority over any adversary. It is critical that information and data passing through and between these systems are secure against any threat or attempt to access, manipulate, or change the data in any way. In addition, these systems are beginning to interconnect with other federal systems outside the purview of DoD.

The DoD and other federal entities have developed differing certification processes and differing test and evaluation requirements to support the certification process. As the need for cross domain interconnectivity increases, the need for more standardized certification test and evaluation processes becomes apparent.

The Joint Applied Project investigates and provides a comprehensive overview of the current Certification Test and Evaluation (CT&E) testing and reporting practices within the National Security Agency. The goal of this project is to identify and document both the process and methodology currently in use during CT&E testing, and to analyze alternative methods to enhance the efficiency and reduce the test duration using a Test Plan Framework.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

I. INTRODUCTION 3
- **A. BACKGROUND 4**
- **B. MOTIVATION 5**

II. BACKGROUND 7
- **A. SECURITY REQUIREMENT AND SECURITY CONTROLS 7**
  - **1. Security Categories 7**
  - **2. Security Controls 8**
- **B. COMPETING RISK MANAGEMENT FRAMEWORK (RDAC AND NIST) 8**
- **C. THE TEST PLAN FRAMEWORK – THE SOLUTION 9**

III. DATA 13
- **A. CT&E TEST PHASE METHODOLOGY – CURRENT STATE 13**
- **B. CT&E TEST PHASE METHODOLOGY – END STATE 18**
- **C. TEST PLAN FRAMEWORK – IMPROVING THE STATUS QUO 19**
- **D. TEST SCENARIO DEVELOPMENT – AN EXAMPLE 20**

IV. ANALYSIS 23
- **A. CURRENT STATE ANALYSIS 23**
- **B. END STATE ANALYSIS 23**
- **C. STATUS QUO ANALYSIS 24**
- **D. SUMMARY 25**

V. CONCLUSION AND RECOMMENDATIONS 27
- **A. CONCLUSION 27**
- **B. RECOMMENDATIONS 27**

LIST OF REFERENCES 29

INITIAL DISTRIBUTION LIST 31

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. RDAC Version 2 10
Figure 2. RDAC Comparison 16
Figure 3. RDAC V2.2 Risk and Threats 17
Figure 4. The Framework 20

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Security Categories 7

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

CASTER	Certification & Accreditation Security Test & Evaluation Repository
CNSSG	Committee on National Security Systems Guidance
CNSSI	Committee on National Security Systems Instructions
CT&E	Certification Test and Evaluation
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DSAWG	Defense IA Security Accreditation Working Group
GOTS	Government off the Self
IA	Information Assurance
IC	Intelligence Community
IV&V	Independent Verification and Validation
NIST	National Institute of Standards and Technology
NMS	National Military Strategy
NSA	National Security Agency
NSS	National Security Strategy
NSS	National Security System
NSTISSC	National Security Telecommunications and Information Systems Security Committee
PoC	Point of Contract
RDAC	Risk Decision Authority Criteria
SABI	Secret and Below Information
SG	Security Categories

TPF	Test Plan Framework
TSABI	Top Secret and Below Information
UCDMO	Unified Cross Domain Management Office
XML	Extensible Markup Language

ACKNOWLEDGMENTS

The author would like to acknowledge and give special thanks to Mr. Brad Naegle and Mr. Michael W. Boudreau for their sound guidance, encouragement, and timely beneficial feedback. Finally, but most importantly, tremendous thanks goes to my family for providing the needed time and support to conduct and to record the project.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

DoD envisions and is currently developing a wide array of System of Systems and Net-centric warfighting systems that interconnect with many platforms and information repositories designed to provide warfighters information superiority over any adversary. It is critical that information and data passing through and between these systems are secure against any threat or attempt to access, manipulate, or change the data in any way. In addition, these systems are beginning to interconnect with other federal systems outside the purview of DoD.

The DoD and other federal entities have developed differing certification processes and differing test and evaluation requirements to support the certification process. As the need for Cross Domain interconnectivity increases, the need for more standardized certification test and evaluation processes becomes apparent.

The Joint Applied Project investigates and provides a comprehensive overview of the current Certification Test and Evaluation (CT&E) testing and reporting practices within the National Security Agency. The goal of this project is to identify and document both the process and methodology currently in use during CT&E testing, and to analyze alternative methods to enhance the efficiency and reduce the test duration using a Test Plan Framework.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

One of the major tenets of both the National Security Strategy (NSS) and National Military Strategy (NMS) is Information Dominance (Obama, 2010). To that end, strategic and tactical information systems have been developed or expanded dramatically over the past decade in the Department of Defense (DoD), Department of Homeland Security (DHS), National Security Agency (NSA), and other Intelligence Community (IC) entities. To leverage these assets across the federal government, systems have been, or soon will be interconnected to share information.

A major concern of these federal information systems is Information Assurance (IA), which can be basically defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. While this is a common concern across federal agencies, the approach for risk management, IA certification, and the supporting test and evaluation processes differs amongst federal entities. These differences create even more problems when attempting to interconnect systems as IA processes and certifications must be maintained in both interconnected 'domains' as well as within the information exchange processes and devices.

When examining the certification and associated test and evaluation standards for potential interconnected, cross-domain systems, additional or differing tests are often required to satisfy the Cross-Domain Solution (CDS) IA standards. This obviously causes delay and additional funding requirements for one or both systems. NSA has been designated as the lead federal agency in setting standards for CDS IA evaluations.

The National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS) issued policy NSTISSP 11, in January 2000 and revised it in June 2003.

> The acquisition of all GOTS IA [Government Off-The-Shelf Information Assurance] and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security

> information shall be limited to products which have been evaluated by NSA [National Security Agency], or in accordance with NSA-approved processes. (NSTISSP 11, 2003, p. 2)

The NSA's Cross Domain Solutions Test and Evaluations Division has developed and formulated policy in conduct of Certification Test and Evaluation (CT&E) testing in support of NSTISSP 11 in the form of handbooks or guides. Discussion of the various documents as they apply to CT&E testing and augmentation by a test plan framework is developed in this research.

A. BACKGROUND

The acquisition of Government-off-the-shelf Information Assurance (GOTS IA) and IA-enabled Information Technology (IT) products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products that have been evaluated by the National Security Agency (NSA), or in accordance with NSA-approved processes (CT&E Handbook, 2009). The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No.11, provides the policy that products shall meet appropriate criteria to ensure integrity and confidentiality of information and also ensuring that authentication and non-repudiation are active during the exchange of electronic data transactions. NSA Cross Domain Solution (CDS) Certification Test and Evaluation (CT&E) Handbook, Version 3.4 (25 August 2006) defines the test objectives required for CDS devices using Security Requirement (SR) categorized into nine test objective derivations. The resulting data feed into the Risk Decision Authority Criteria (RDAC), which provides a method to measure the risk of CDS implementation and a method for making a connection decision by the Defense Information Systems Network (DISN) connection approval authorities for a CDS implementation. In an effort to improve sharing of information objectives between the Department of Defense (DoD) and Intelligence Community (IC), the Unified Cross Domain Management Office (UCDMO) was chartered in March 2007. Additionally, this office chartered a Community Security Testing Group (CSTG) with a primary mission to develop test readiness requirements and test objectives that can be interchanged, and

using reciprocity, can be applied to both DoD and the IC CDS requirements. The CSTG has recommended CDS security controls for inclusion into the National Institute for Standards and Technology (NIST) Special Publication (SP 800-53) to improve reciprocity and standardize common controls during CT&E testing. Adoption of these security controls by DoD, IC, and NSA will ultimately streamline and reduce the exorbitant cost of the CT&E conduct. Implementation of these security controls requires tailoring of the discrete security controls for the particular type of cross-domain solution placed under test. While it may be a simple matter to tailor these security controls for a particular test, a test plan is the ideal vehicle to codify the selected controls and provide a plan of instruction to enable a consistent test environment for all labs involved in testing CDS security products. Thus, a common master test plan framework would enable and provide efficiency to the overall process of vetting and validating CDS, while simultaneously providing rigorous security testing to minimize vulnerabilities for the user communities.

B. MOTIVATION

Testing of CDS devices requires detailed understanding of security categories and processes that investigate the efficacy of protecting data or traffic flow between differing security enclaves. Current testing methodology is deficient in providing fiscal and test duration savings. The inclusion of a test plan framework will allow for a more streamlined approach for the current test methodology to recognize the impact of the security controls and the RDAC Risk Management Framework as it applies to both fiscal and schedule constraints. Current test methodology uses security controls developed, with the cooperation with NIST and NSA, that are tailored to the CDS type under test. These security controls, however, are not detailed enough to provide a step-by-step test scenario. Further tailoring and discussions between the test lab and the NSA point-of-contact are required to identify the appropriateness of a particular security control for the device under test. These discussions normally occur during the conduct of the test, which may impact schedule and funding of the test effort. The inclusion of a test plan would avoid these additional tailoring functions as the plan would provide the necessary

information at the start of the test, not during the testing phase, which would likely be disruptive to the schedule and add to testing costs. This research recognizes that the testing process should be planned, given valid security controls and sufficient tailoring of these controls, to affect a timely and completed analysis of test results that are used to provide a risk rating using the RDAC methodology.

Research methodologies used in the development of this Project relied on existing documents and regulations. Current processes were inspected in view of documentation that was in draft or had outdated status. In addition to the volume of existing documentation, the CASTER software program was investigated to fulfill a need for more efficient testing by the introduction of the test plan framework.

II. BACKGROUND

A. SECURITY REQUIREMENT AND SECURITY CONTROLS

1. Security Categories

The Cross Domain Solution (CDS) Certification Test and Evaluation (CT&E) Handbook developed and published by NSA I123 Directorate, defines the test objectives required for CDS devices using Security Categories (SGs). (CT&E Handbook) The following table enumerates these security categories. With a shift in testing methodology, security controls finalized in NIST SP 800-53 rev. 3 and CJCSI 6211.02C are now used as input to RDAC. Documentation to implement this shift is currently in draft and expected for final release during 2010.

Table 1. Security Categories

Category	Requirement Label
SR1	Documentation
SR2	Configuration Management
SR3	Local Base System Security
SR4	Remote Access Control
SR5	Data Flow Configuration & Review
SR6	Content Filtering Verification
SR7	System Integrity
SR8	Stress Testing
SR9	Penetration Testing

A guard is designed to ensure secure data sharing between networks of differing classifications and to provide protection against the loss of classified data or introduction of malicious code into the classified network. To verify the secure transfer of data by the guard, a set of nine Security Categories (SGs) were developed. These SRs were initially derived from a review of:

- Common Criteria high-assurance characteristics
- Previous assessment reports for the Secure Network Server (SNS) and Defense Information Infrastructure (DII) guards
- DoD 8500.1 Information Assurance [Canceled DoD 5200.28-STD] and DoDI 8500.2 Information Assurance Implementation

The results of testing against the SRs are to create a body of evidence that can be used to perform a risk assessment of the CDS to determine its appropriateness for the proposed implementation. These results of the CT&E, or body of evidence, will identify potential weaknesses that can be corrected or mitigated to attain a secure CDS. Each SR is comprised of rationale statements with further explanation of how the SG should be tested during a CT&E and then translated into test procedural requirements used in writing specific tests.

2. Security Controls

Security Controls developed with the creation of the UCDMO under a charter signed by both the Assistant Secretary of Defense for Network Information Integration (ASD NII) / Department of Defense Chief Information Officer (CIO), and Associate Director of National Intelligence Chief Information Officer. The National Institute of Standards and Technology (NIST), in concert with the UCDMO, developed a standard set of security controls specifically tailored for CDS that allow all federal government organizations to establish a baseline for testing to allow for reciprocity in acceptance of CT&E results for all tests. NIST Special Publication 800-53, Information Security, recommends security controls that can be tailored for the different type of CDS devices and the associated deployment environment. The DoD community is expected to adopt NIST SP 800-53 by the summer of Fiscal Year 2011 (FY11) and replace the current DoD Information Assurance Certification and Accreditation Process (DIACAP) security categories.

B. COMPETING RISK MANAGEMENT FRAMEWORK (RDAC AND NIST)

NSA's Risk Decision Authority Criteria (RDAC) Version 2.2 describes methodology for risk certifiers to summarize and to identify risks associated with the CDS devices. The criteria provide a way to recommend acceptable levels of risk, as well as to consider how those risk factors can be traded off against each other. The criteria are not only intended for use by accrediting agents resolving complex mission-versus-risk issues, but they can also be used during initial analysis of a cross domain requirement.

Because the RDAC takes an architectural approach to analysis, best-case risk analysis can be performed prior to formal testing and be considered when determining whether to expend resources testing new or updated CDS technology.

Another approach of risk management is the NIST Risk Management Framework which uses a security life cycle approach. NIST SP 800-59, Security Categorization provided guidelines for identification of Information Systems as a National Security System (NSS). National Security Systems are defined as using functions such as intelligence operations, involving cryptographic activities, command and control systems, equipment that is integral or part of a weapons system, and is critical to the direct fulfillment of a military or intelligence mission.

Both the RDAC and the NIST approach identify risk associated with the CDS devices. NIST uses Impact Categorization for the security aspects of risk, it does not provide a structure for the Operational Impact of accreditation decisions or the "enterprise risk" objective of the C&A Transformation Risk Executive Function. RDAC, however, was developed for the collateral DISN, the Defense IA Security Accreditation Working Group (DSAWG), and DISN Flag Panel to assist in the decision-making process on whether to allow a cross-domain connection.

C. THE TEST PLAN FRAMEWORK – THE SOLUTION

Cross Domain Solution testing requires a significant preparation phase prior to engaging the test team. Current documentation emphasizes the risk analyses as a solution to test planning, however, the lack of a test plan framework creates an ad-hoc test scenario mostly driven by NSA's point of contact assigned to the laboratory that executes the test. The current implementation of RDAC is used as a model to fill in the necessary test scenarios as a mechanism to evaluate the risk for a particular assigned risk element. Technical and Data risk are two elements required for CT&E testing and are further decomposed into threat groups. These groups are then segregated into technical, preventative, and detective facets. Certification & Accreditation Security Test & Evaluation Repository (CASTER), the automated test repository, uses the RDAC facets

to develop test scenarios that can be stored and retrieved from a master database to ensure coverage is complete for each assigned test. The CASTER software has not been updated to reflect the current RDAC 2.2, but uses the superseded RDAC 2. The hierarchy is described in figure 1. Note that the CASTER software only addresses the right hand side of the diagram.

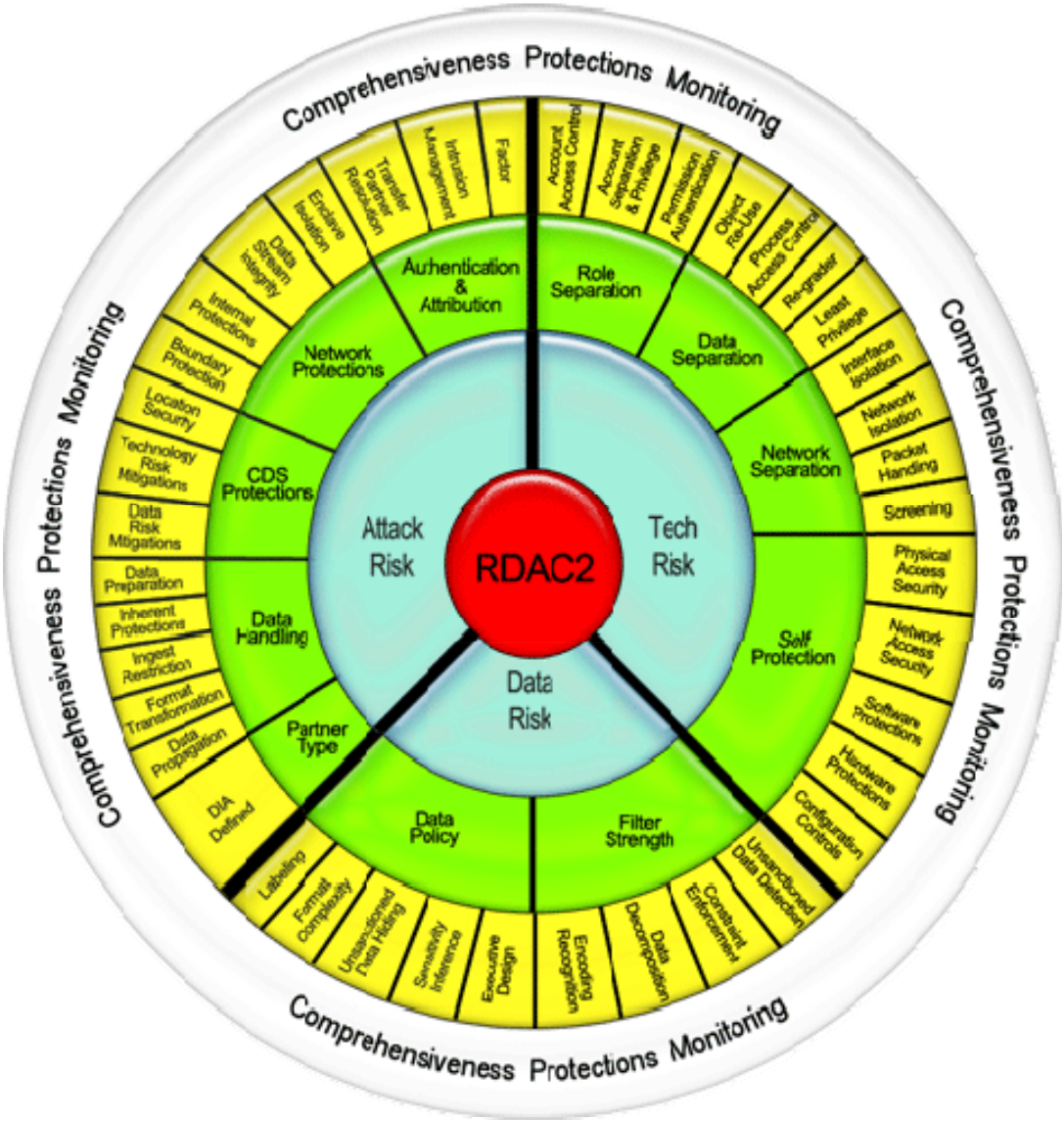


Figure 1. RDAC Version 2

The determination on how many and what types of test scenarios are required is decided by the NSA POC as the test is being executed. This process introduces ad-hoc interpretation of the amount of testing required to satisfy the risk threat and thus, affects the test schedule and associated costs. The introduction of a Test Plan Framework (TPF) would likely provide the necessary structure to map out the required tests that both satisfy the RDAC requirement and also ensure that sufficient test data is collected. The purpose of the TPF is to provide a definitive structure and methodology that promotes uniformity in test scenarios and allows for a better report output that is fed into the RDAC assessment. The remainder of this document explains how the TPF is integrated into the current overall test methodology to ensure complete and consistently valid test results that are the basis for risk assessment and ultimately, provide for connection approval of the CDS.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA

A. CT&E TEST PHASE METHODOLOGY – CURRENT STATE

Complete and efficient testing of Cross Domain Solution devices relies on processes and methodologies that are currently in a state of flux. The Cross Domain Solution (CDS) Certification Test and Evaluation (CT&E) Handbook Version 3.4 was last updated in August 2006, and sets forth processes and procedures used in the conduct of the test evaluation.

> The purpose of this document is to provide the independent government labs with a structured, repeatable approach to assess the security and functional features of a CDS. Because CDSs are used to transfer data between networks of differing classifications, a high degree of trust is placed in their ability to protect the network of higher classification from attack and to prevent the accidental release of classified data to the network of lower classification. The CT&E process defined in this document provides the methodology for independent testing and evaluation of a particular CDS. (CT&E Handbook Ver. 3.4, 2006, p. 9)

Other documents and software applications that are utilized during testing are the Risk Decision Authority Criteria Implementation Guide, Version 2.2, and the Certification and Accreditation Security Test and Evaluation Repository (CASTER) software program. CASTER implements the risk criteria requirement to ensure that all required testing satisfies and enables an RDAC rating. The CT&E handbook further describes four phases that are used in performance of a test event.

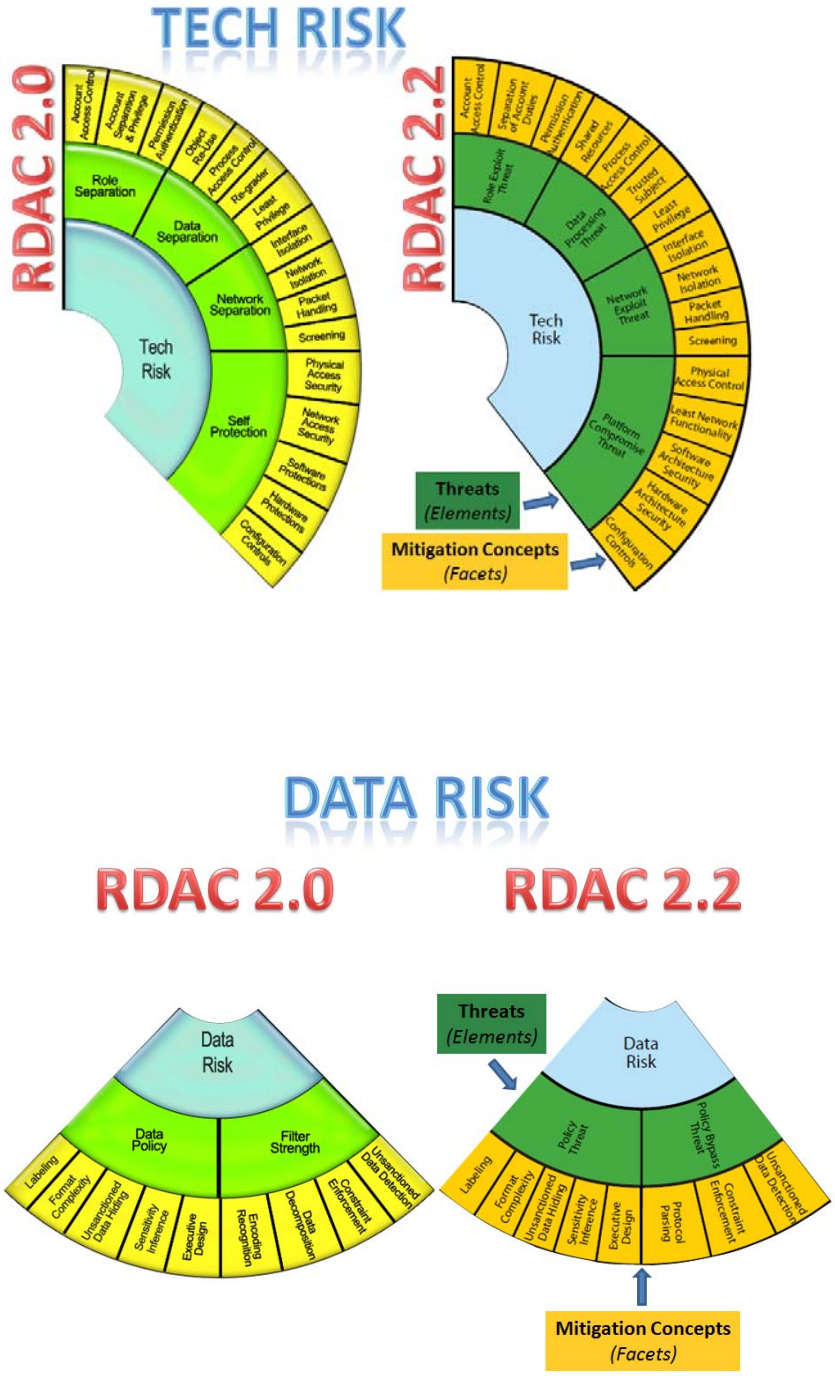
- The Planning Phase consists of identifying the cost, schedule, and scope of the CT&E, establishment of the CT&E team, and defining the various roles and responsibilities for the test process (CT&E Handbook Ver. 3.4, 2006, p. 16).
- The Preparation Phase consists of establishing the lab environment, continuing familiarization with the CDS, and beginning the development of the CT&E test objectives using the Certification and Accreditation Security Test and Evaluation Repository (CASTER) (CT&E Handbook Ver. 3.4, 2006, p. 25).

- The Testing Phase includes identifying the guidelines for classifying documents, media, or equipment, defining individual test procedures for each test objective, dry running the test procedures, defining and accomplishing the formal testing, and documenting the test results in CASTER (CT&E Handbook Ver. 3.4, 2006, p. 55).
- The final phase is the Results Phase, which includes making risk level determinations for each of the findings, determining possible countermeasures and recommendations, completing the CDS CT&E Report, and coordinating the final document through the CDS Requirements and Evaluations Division (CT&E Handbook Ver. 3.4, 2006, p. 60).

The draft CT&E Handbook updates the nine security requirements in Table 1 and replaces them with a catalog of security controls defined in NIST SP 800-53. The CASTER software is being updated to take advantage of the security control as defined in SP 800-53. Until completed, the current testing efforts remain in differing states of testing methodology. This differing state of testing is demonstrated by the latest test effort for Project Manager (PM) Brigade Combat Team Modernization (BCTM), which uses the security requirement testing methodology as defined in the CT&E Handbook Ver. 3.4 and the test data application CASTER uses the RDAC version 2 risk criteria. Ideally, the methodology should represent the latest risk and testing criteria as defined in the CT&E Handbook Ver. DRAFT 2009 and the current Risk Decision Authority Criteria Version 2.2.

The RDAC was developed by the National Security Agency in 2002 by the System and Network Analysis Center (SNAC) of the National Security Agency (NSA) at the request of the Defense Information Systems Network (DISN) Flag Panel, who is ultimately responsible for the accreditation and connection approval for CDS devices. RDAC has been implemented within the collateral DISN community since 2003, and from 2003 thru 2007, RDAC 1.2 was the version in use. In 2007, two high-level reasons for updating the criteria from their original specification were incorporated into RDAC. These changes where implemented to provide finer granularity in conveying risk and

secondly, to improve the connection approval process for DISN community networks. The Risk Decision Authority Criteria Version 2.2 has replaced Version 2, as shown in Figure 2.



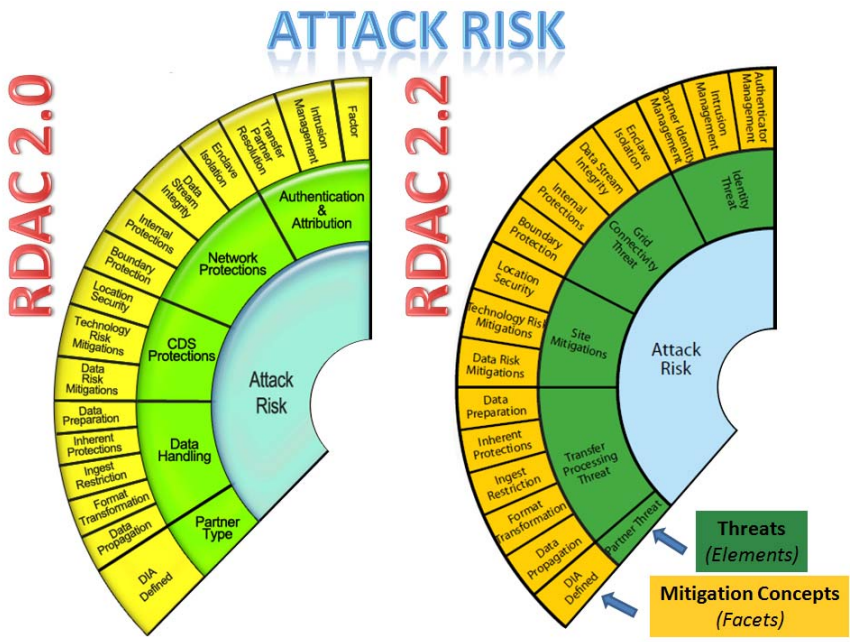


Figure 2. RDAC Comparison

Only half of the RDAC wheel is applicable to the test methodology of the CT&E as the other half describes risk associated with non-technical issues for CDS devices. The new RDAC described in the RDAC Criteria v2.2 model updates the weight of the threat model roll-up, adds an access solution criteria chart, solidifies quality granularity, and filter strength. An access solution criteria chart was added in order to address approval concerns with an access solution CDS. Quality granularity was improved by implementing a fourth choice for technical implementation in order to force subject matter experts to select a value and not to "stay on the fence" (as cited in RDAC Criteria v2.2, p. 9). Lastly, filter strength was improved by reducing the number of mitigation concepts from four to three. The risk assignment methodology of RDAC is partially implemented using the prior RDAC release in the CASTER database application. The actual assignment of risk is accomplished independently of the CT&E assessments and is not discussed in this document.

RDAC v 2.2 establishes three risks that must be analyzed: Technology Risk; Data Risk; and Attack Risk. Attack Risk and Data Risk, with the exception of Policy Threat, is not tested during CT&E, but is evaluated by NSA separately. Figure 3 shows the relationship between risks and threats (CT&E Handbook, Ver. 4.0 Draft, 2009, p. 100).

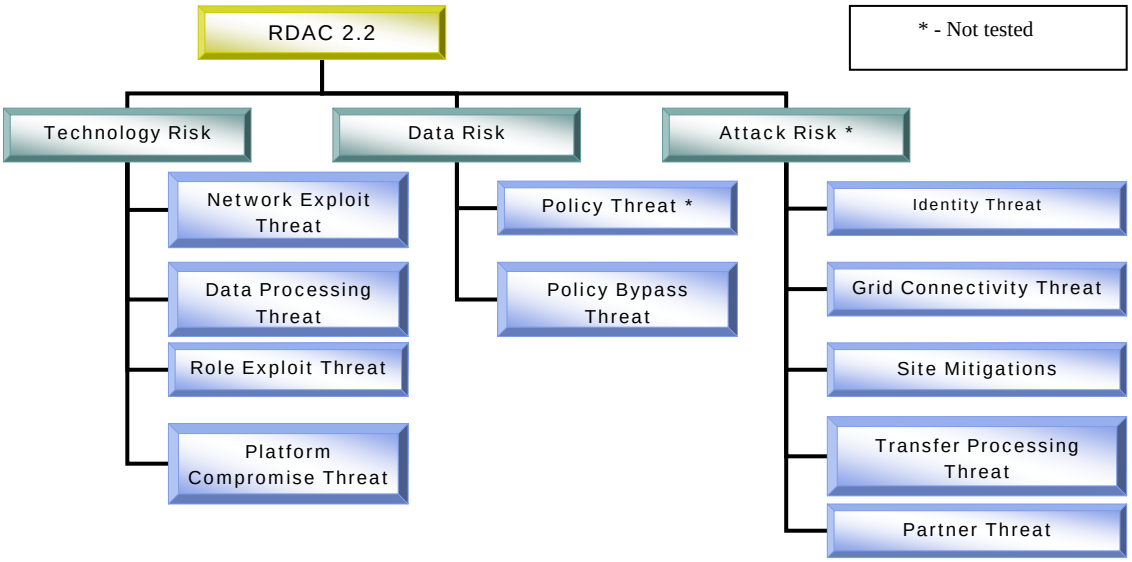


Figure 3. RDAC V2.2 Risk and Threats

Technology Risks, together with the Policy Bypass Threats part of Data Risk, provide the core of CT&E testing. The four threats that make up the Technology Risk are Network Exploit Threat, Data Processing Threat, Role Exploit Threat, and Platform Compromise Threat, all of which are discussed below.

- Network Exploit Threat, this type of threat indicates a level of assurance that the CDS device or platform adheres to the Open System Interconnection (OSI) stack.[1] Additionally, separation of data is enforced to ensure that transfers are permitted to the connected networks at the physical, data link, network, and transport layers of the OSI stack.

[1] Open System Interconnection (OSI) defines a networking framework model that implements protocols in seven layers, where control is passed in sequence from layer to layer. Retrieved 10 May 2010 from Webs ite http://www.webopedia.com/quick_ref/OSI_Layers.asp.

- The Data Processing Threat is an indication how the CDS platform distinguishes data that is moved between security domains and provides appropriate security labeling when data is moved or transferred as defined in policy.
- The Role Exploit Threat used the concept of least-privilege, so that changes affecting the CDS are monitored and recorded according to the defined security features and functions.
- The final threat under Technology Risk is the Platform Compromise Threat that indicates a level of difficulty when configuration changes are made to the CDS regardless of whether they were authorized or not.

The Policy Bypass Threat, part of the Data Risk assessment, measures the filtering mechanism of the CDS. These filters are designed to provide an effective implementation of a filter policy that permits regulation of data flow between security domains (CT&E Handbook, Ver. 4.0 Draft, 2009, pp. 100–103).

The Attack Risk, as noted in Figure 3, measures the likelihood of both the risk of the environment into which the CDS is implemented, as well as the likelihood that the environment that the CDS is placed can be successfully exploited. The Policy Threat part of the Data Risk provides for specifications of the data payload passing through the CDS, while the Policy Bypass Threat verifies that data.

B. CT&E TEST PHASE METHODOLOGY – END STATE

Alignment of documentation and software in conduct of the CT&E is of paramount importance. The documentation must assist in providing the necessary structure and guidance to testers in order to provide a comprehensive body of evidence that has validity in determining, together with other risk factors, whether the accrediting agents have sufficient information to provide a connection approval for the CDS device. Connection approval is the final hurdle that a program manager or sponsored system developer must obtain to either connect, or place the CDS device on the approved product list.

Ideally, the CT&E Handbook is the entry point document for the CT&E testing organization. Thus, it must reflect current processes and guidance as developed by NSA and the UCDMO. Prior testing of any CDS device, by the test organization, must have undergone a vetting process that ensures that the product is ready for test. This initial entry requirement prevents a product under test from being in a constant state of modification. Testing of this nature is conducted during the Independent Verification and Validation (IV&V) testing phase. The current CT&E Handbook Version 4.0 is in the draft stages to improve the process of defining test objectives. The security controls, as specified in NIST SP 800-53, CNSSI 1253, and CNSS 1253A, are used in conjunction with the Unified Cross Domain Management Office's (UCDMO) CDS Profile Tool. The CDS Profile Tool is available, at request, from the UCDMO and provides an initial assessment using the NIST SP 800-53 control, tailored to the type of CDS device under test. CASTER currently uses the security controls to assist the test community in ensuring that all required test scenarios are completed and that sufficient information is collected to provide a body of evidence. This evidence body is fed into a report and is used as a partial basis in determining connection approval by the DISN Flag panel. Responsibility for allowing the connection between different security domains is determined by the body of evidence created thru the CT&E testing process. Without approval of the Authority to Operate (ATO), the CDS device is not allowed to be used to mediate or process data on both sides of the security enclaves, rendering it useless in a CDS environment.

C. TEST PLAN FRAMEWORK – IMPROVING THE STATUS QUO

Numerous regulatory policies, handbooks, and guidance documents, appear to conflict and thus, affect test processes. The necessity of creating a test plan framework is apparent to ensure consistent and repetitive CT&E test results. Lack of a test framework causes confusion, can lengthen the test period and can also impact master schedules and budgets in the overall development of CDS devices. The creation of a test plan framework will improve the test methodology by ensuring that the test plan is tailored for a particular type of CDS, and together with guidance of the latest CT&E handbook and

risk guidance documents, provides a consistent result that can be used by the test community to ensure consistent testing processes and methods. The proposed test plan framework uses these existing documents as shown in Figure 4.

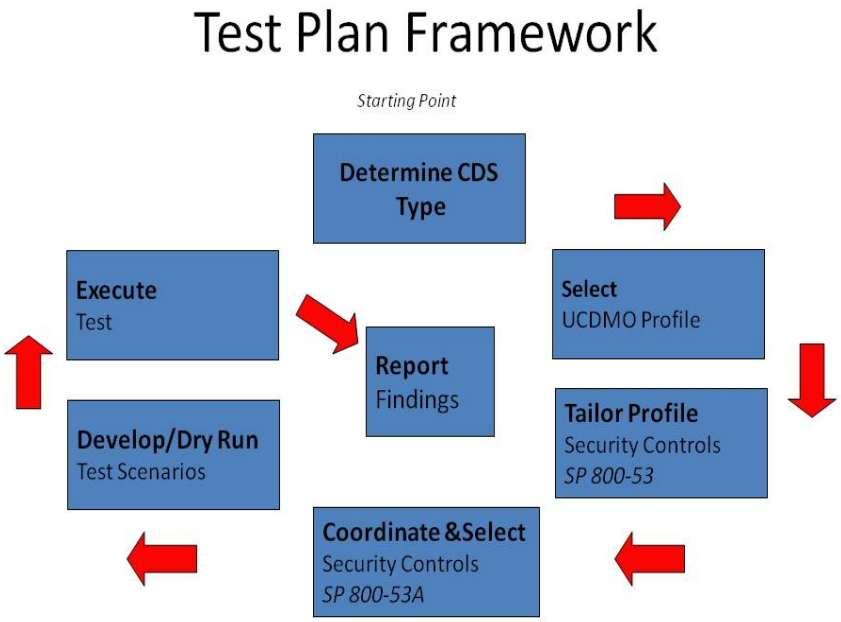


Figure 4. The Framework

The proposed test plan framework forces the participants to select a methodology that streamlines and ensures that the CDS under test uses the appropriate security controls. This framework allows development of a CDS test plan that is complete and addresses all security concerns in a systematic and controlled manner. The ultimate reason to test CDS devices is to discover and document vulnerabilities so that their associated risk can be identified, corrected, or managed.

D. TEST SCENARIO DEVELOPMENT – AN EXAMPLE

Initial guidance for test scenario development is outlined in the Cross Domain Solution Certification Test and Evaluation Handbook. The handbook uses a phased approach in the conduct of the CT&E. The phases are as follows:

- Planning Phase – Assignment of roles, responsibilities, and working relationship between the Test Team, Vendor, and NSA PoC

- Preparation Phase – Familiarization and CDS baseline installation; test objective development

- Testing Phase – Define test procedures for each test objective; verify and test for record

- Results Phase – Provide comments, vulnerabilities, and countermeasures; assign Collective Statement of Risk; provide the CDS CT&E report.

Of the four phases, the preparation phase is the most critical to the success of the CT&E. Test procedures are created to provide a repeatable, step-by-step approach to validate the test objective. The test procedures should be in sufficient granularity to afford repeatability and consistency in the test results. Testing should also consider both negative and positive aspects, thus ensuring complete testing of the provided security functions of the CDS. Tailoring the test objective for a particular CDS device requires agreement between the test element and the NSA PoC. The tailoring of objectives is currently being developed to assist in providing a consistent number of pertinent test objectives that will satisfy the RDAC risk criteria. CASTER is the default database application tool used in the conduct of the CT&E test and is the repository of test results and associated reports used in the risk analysis for ultimate connection approval to DoD and other federal networks. The objectives from the Preparation Phase are loaded into the CASTER database and linked to the test procedure template, then displayed visually to the tester. The example test objective, below, selected to illustrate the testing process, reflects how the system implements the audit requirement for password failures.

- Test Objective: Ensure that the system provides a mechanism to audit password failures.

- Test Procedure development:

    - Ensure the CDS is in a known default state (from Preparation Phase)

        - Step 1: At the system login prompt, login as *a normal user*

            - Expected Result: System requests *password*

- Step 2: Enter an incorrect password
    - Expected Result: *"Password is incorrect- try again"*
- Step 3: Enter the incorrect password again
    - Expected Result: *"Password is incorrect- try again"*
- Step 4: Enter the incorrect password again
    - Expected Result: *"Account Locked – contact System Administrator for Access"*
- Step 5: At the system login prompt, login as *root* (administrator)
    - Expected Result: System requests *password*
- Step 6: Enter correct password
    - Expected Result: *root* is logged in and terminal is accessible
- Step 7: Enter the command: {*grep "password" /var/audit/audit.log | grep "locked"}*
    - Expected Result: *grep* returns the record from the log that shows that the account is in lockout status for the user
- Step 8: The final step normally restores any changes back to default and readies the system for the next test.

o When this test is executed for record, the CASTER application provides the following result flags: Passed; Failed; Passed with Comment; and Not Tested. All flags, except the "Passed" flag must be addressed in view of vulnerabilities and mitigation of the risk of failure.

This simple example demonstrates the amount of detail that is required to ensure that the test is repeatable and produces consistent results.

IV. ANALYSIS

A. CURRENT STATE ANALYSIS

The Cross Domain Solution Certification Test and Evaluation Handbook Version 3.4 last published in 2004, does not reflect current test processes that can be used by the independent government laboratories to provide "a structured, repeatable approach to assess the security and functional features of a CDS" (CT&E Handbook Ver. 3.4, 2006, p. 9). One of the major changes in testing of CDS devices is the replacement of the Security Requirements 1 thru 9 as depicted in Table 1, with the risk criteria stated in the Risk Decision Authority Criteria Version 2.0. This change was effected via CASTER, a software database program, which provides the necessary mapping processes to enable the testers to map the nine security categories to risk elements. Modification to CASTER's database structure uses the risk elements as testing criteria to ensure that all necessary security questions are answered in order to perform an accurate risk assessment.

The current CDS risk and testing guidance uses outdated policy and guidance documents, especially the CT&E Handbook. Revision of this handbook is now in draft, with an expected release date during 2010. The only current guidance is RDAC Version 2.2, which improves on RDAC Version 2.0 by aligning risk with threat elements, allowing risk values to support more granularity and therefore, provide a better risk assessment. Additional modification to the CASTER software to reflect the latest changes to RDAC is being discussed by the developers with input by the independent labs and NSA. Until documentation and processes are aligned to reflect a robust testing methodology, the independent tester will continue to struggle with ad hoc guidance from the NSA PoC in conduct of the CT&E test.

B. END STATE ANALYSIS

The entry point for CT&E testing is the CT&E Handbook as it provides guidance in the performance of the CDS test. The draft CT&E handbook, currently in the staffing

phase, is being rewritten to reflect the current testing methodology and incorporates changes brought about by the creation of the UCDMO. Reciprocity of test results between the DoD and IC communities has been the UCDMO's greatest challenge. UCDMO, in concert with NSA, DoD, and NIST, are developing methods and processes that can produce a consistent body of evidence by the independent labs and the IC community lab for testing of CDS devices, both in the Secret and Below Information (SABI), and Top Secret and Below Information (TSABI) environments. Ideally, testing should be tailored to address security categories that cover both environments to reduce the costs involved in test duplication or additional testing for the different environments. In the final state, the TSABI and SABI risk analyses will merge, thus simplifying the risk analysis that is used in determining connection approval by the DISN Flag panel.

Documents that provide further guidance to the test community are being revised and published to ensure that the security categories are being addressed in a repeatable process. CNSSG 1253A is a companion guideline to the Security Controls Catalog for National Security Systems (CNSSI 1253). CNSSI 1253 covers the steps in the Risk Management Framework that address security control selection and determines what security controls are needed to protect security information, in accordance with the security categories presented in Security Categorization for National Security Information and Information Systems (CNSS Instruction 1199). CNSSG 1253A covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance in building and managing the assessment results.

C. STATUS QUO ANALYSIS

The lack of an overarching framework for the testing community introduces duplication, lack of consistent and repeatable results, and increases the cost for the user community in today's constrained funding environment. Documents that are outdated must be updated, software programs used in the conduct of the CT&E must reflect current test methodology, and the establishment of a testing framework should be created

to assist in providing the development of a test plan that allows for a robust, repeatable, and more universally acceptable body of evidence by the testing community.

D. SUMMARY

New file formats, such as the Open Document Formats (ODF), Extensible Markup Language (XML) variants, Adobe Portable Document Format (PDF) and the latest versions of the Microsoft Office document formats, encourage the design of cross domain devices to allow for the sharing of information between security domains. Simple text files of the past, which use the ASCII[2] encoding schema, have been relegated for use in computer language development and scripting applications. These ASCII text files are easily parsed and tested for illegal or malicious security content. Other complex file types have the capability to include metadata, thus increasing the risk of containing embedded code that may have malicious intent. Image and video files can also contain hidden text and active code programs, such as Microsoft's ActiveX or Sun's JAVA. These active code programs can provide a vector mechanism to infect the latest file formats. The current CDS devices must keep pace preventing and protecting against security transfer leakage, and detect and prevent malicious/virus code, including the detection of defined code words from traversing the security domains.

The creation of a Test Plan Framework will provide the necessary guidance to define test processes and scenarios using a comprehensive test plan that can be shared with the test community to reduce schedule and costs. Additionally, the framework identifies all required documents and processes required during the conduct of the CT&E. Creation of this Test Plan Framework will enable a more structured approach to testing CDS devices and avoid questions that should have been answered during testing but where discovered after testing was completed. Although CT&E testing provides part of the input to the final risk assessment, it is critical that the testing covers all pertinent security categories to provide a body of evidence for those that must make a decision to connect or not connect the CDS to the existing cross-domain network infrastructure.

[2] ASCII – American Standard Code for Information Interchange is a character-encoding scheme.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

Processes defined in the conduct of the CT&E are not clearly stated and can negatively impact the results of the CDS testing phase. The use of ad hoc or poorly defined objectives to arrive at a risk assessment reveals inconsistencies in the body of evidence. Since the result of this body of evidence determines, to some extent, the risk of the cross domain solution, it is imperative that the information collected be based on a risks-based plan. Handbooks and other guidance documents by themselves, do not guarantee efficient testing. Planning and tailoring the security requirement of the CDS under test provides an opportunity for better risk assessment, supporting the ultimate approval by the DISN Flag panel.

B. RECOMMENDATIONS

The creation of a Test Plan Framework that requires all participants to engage the testing community prior to any actual equipment testing is a solution that will improve the testing process by requiring that an approved Test Plan be provided as a key driver for a successful CT&E. The Test Plan Framework, shown in Figure 2, details key items that must be addressed for a successful CT&E. These key items include:

Determining the CDS type:

This determination is provided by NSA and consists primarily of two-way or one-way Directional CDS devices. Data is restricted by policy or filter mechanisms.

Selecting the UCDMO Profile:

The profile considers the Security Controls in SP 800-53, which are specifically tailored for the CDS under test. This profile provides a first cut of security control items that may apply to the test event.

Tailoring the Profile:

Once a profile has been selected, further tailoring focuses on the criticality of controls. Other security controls that have not been identified in SP 800-53 and SP 800-53A are included in the modified profile (NIST SP 800-53A, 2008, p. 14).

Coordinating and Selecting the Security Controls:

Using SP 800-53A to help identify any other test detail (with the NSA POC) that are required to completely test the security control as it applies to RDAC (NIST SP 800-53A, 2008, p. F5 – F288).

Developing and Validating Test Scenarios:

Development of test scenarios or procedures using the selected security controls and exercise of the procedures is accomplished during this phase.

Executing the Test:

The test procedures are execute and recorded.

CT&E Reporting:

A final CT&E test report should be developed using the test artifacts and associated results. Results of the report provide an improved method to arrive at a CDS risk assessment using RDAC guidelines.

The Test Plan Framework is the enabler to ensure that the accrediting agents have the necessary risk analyses to make the ultimate decision to connect, or not connect the CDS device to the network. After all, the security of the network infrastructure is determined by the weakest link in the chain, or in this case, the most vulnerable Cross Domain Solutions device that is interconnected.

LIST OF REFERENCES

Committee on National Security Systems. (2009). *Security Categorization and Control Selection for National Security System* (CNSS Instruction No. 1253 Ver. 1). Retrieved May 2010 from http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf

National Security Agency. (2003). *National Security Telecommunications and Information Systems Security Policy* (NSTISSP No. 11). MD. Retrieved May 2010 from http://www.niap-ccevs.org/nstissp_11_revised_factsheet.pdf

National Security Agency. (2006). *NSA Cross Domain Solution (CDS) Certification Test and Evaluation (CT&E) Handbook Ver. 3.4.* (Available from the NSA Cross Domain Solutions Test and Evaluations Division).

National Security Agency. (2009). *NSA Cross Domain Solution (CDS) Certification Test and Evaluation (CT&E) Handbook Version 4, Draft.* (Available from the NSA Cross Domain Solutions Test and Evaluations Division)

National Security Agency. (2009). *Risk Decision Authority Criteria.* (RDAC, Ver. 2.2 Draft).

National Security Agency. (2009). *Risk Decision Authority Criteria Implementation Guide*. (RDACI Ver. 2.2).

National Institute of Standards and Technology. (2008). Guide for Assessing the Securi*ty Controls in Federal Information Systems* (NIST Special Publications 800-53A). Retrieved May 2010 from http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf

National Institute of Standards and Technology. (2007). *Recommended Security Controls for Federal Information Systems* (NIST Special Publications 800-53, Rev. 2). Retrieved May 2010 from http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

Obama, B. (2010). *National Security Strategy*. Retrieved May 2010 from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Unified Cross Domain Management Office. (2009). *UCDMO Profile Tool* [Computer Software]. Adelphi, MD.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California