DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) SURVEY AND DECISION TREE

WHITE SANDS MISSILE RANGE
   REAGAN TEST SITE
   YUMA PROVING GROUND
   DUGWAY PROVING GROUND
   ABERDEEN TEST CENTER
   ELECTRONIC PROVING GROUND

NAVAL AIR WARFARE CENTER WEAPONS DIVISION, PT. MUGU
NAVAL AIR WARFARE CENTER WEAPONS DIVISION, CHINA LAKE
NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION, PATUXENT RIVER
NAVAL UNDERSEA WARFARE CENTER DIVISION, NEWPORT
PACIFIC MISSILE RANGE FACILITY
NAVAL UNDERSEA WARFARE CENTER DIVISION, KEYPORT

30TH SPACE WING
45TH SPACE WING
AIR FORCE FLIGHT TEST CENTER
AIR ARMAMENT CENTER
ARNOLD ENGINEERING DEVELOPMENT CENTER
BARRY M. GOLDWATER RANGE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

DISTRIBUTION A: APPROVED FOR PUBLIC RELEASE
DISTRIBUTION IS UNLIMITED
**DoD Information Assurance Certification and Accreditation Process Survey and Decision Tree**

*Puts forth "common" IA practices to include a decision tree for interpretation and implementation of IA.*

**DIACAP; Data Sciences Group; information assurance; IA**

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT unclassified</td>
<td>Same as Report (SAR)</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>b. ABSTRACT unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. THIS PAGE unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Approved for public release; distribution unlimited
This page intentionally left blank.
RCC DOCUMENT 173-11

DIACAP SURVEY AND DECISION TREE

July 2011

Prepared by

DATA SCIENCES GROUP
(DATA PROTECTION COMMITTEE)

Published by

Secretariat
Range Commanders Council
U.S. Army White Sands Missile Range
New Mexico 88002-5110
# TABLE OF CONTENTS

**PREFACE** ...........................................................................................................................................v

**ACRONYMS** ................................................................................................................................ vii

**CHAPTER 1: INTRODUCTION** .........................................................................................................1-1
  1.1 Survey .................................................................................................................................. 1-1
  1.2 Decision Tree ....................................................................................................................... 1-1

**CHAPTER 2: SURVEY AND BEST PRACTICES** .............................................................................2-1
  2.1 Methodology ......................................................................................................................... 2-1
  2.2 Lessons Learned .................................................................................................................. 2-1
  2.3 Best Practices ....................................................................................................................... 2-2

**CHAPTER 3: DECISION TREE AND RECOMMENDATIONS** ......................................................3-1
  3.1 Decision Tree ....................................................................................................................... 3-1
  3.2 Recommendations ............................................................................................................... 3-1

**CHAPTER 4: REFERENCES** .........................................................................................................4-1
  4.1 Federal .................................................................................................................................. 4-1
  4.2 DoD ........................................................................................................................................ 4-2
  4.3 Navy ..................................................................................................................................... 4-4
  4.4 Air Force ............................................................................................................................... 4-4
  4.5 Army ..................................................................................................................................... 4-4
  4.6 Range Specific ...................................................................................................................... 4-5
  4.7 Other: Web Links .................................................................................................................. 4-5
  4.8 Other: RCC References ......................................................................................................... 4-5

**APPENDIX A: DIACAP BACKGROUND INFORMATION** ............................................................ A-1
PREFACE

This document presents the results of efforts undertaken by the Range Commanders Council (RCC) Data Sciences Group (DSG) for completion of Task DS-02, DoD Information Assurance Certification and Accreditation Process (DIACAP) Survey and Decision Tree. The intent of this document is to ensure synergy across the armed forces to allow Information Assurance (IA) continuity by using the best range practices to support the warfighter.

The information contained herein will assist those responsible for oversight of information systems with planning and execution of DIACAP. This document is aimed at addressing any impacts on Range activities in a proactive manner.

For development of this document, the RCC gives special recognition to:

**Task Lead:** Mr. Jim Bulloch  
Member, Data Sciences Group (DSG)  
Pacific Missile Range Facility (PMRF)  
Code N65-4, PO Box 128  
Kekaha, HI 96752-0128  
Phone: (808) 335-4186  DSN (315) 421-6290  
Fax: (808) 335-4980  DSN (315) 421-6980  
E-mail: jim.bulloch@navy.mil

Please direct any questions to:

Secretariat, Range Commanders Council  
ATTN: TEDT-WS-RCC  
1510 Headquarters Avenue  
White Sands Missile Range, NM 88002-5110  
Phone: (575) 678-1107  DSN 258-1107  
Fax: (575) 678-7519  DSN 258-7519  
E-mail: usarmy.wsmr.atec.list.rcc@mail.mil
This page intentionally left blank.
ACRONYMS

ALTD Alternate Tag and Data
APMS Army Portfolio Management Solution
ATO authorization to operate
C&A Certification and Accreditation
CA Certifying Authority
CARS Cyber Asset Reduction and Security
CIO Chief Information Officer
CVC Compliance and Validation Certification
DAA designated accrediting authority
DATO denial of authorization to operate
DIACAP DoD Information Assurance Certification and Accreditation Process
DIP DIACAP Implementation Plan
DITPR DoD Information Technology Profile Registry
DITSCAP DoD Information Technology Security Certification and Accreditation Process
DoD Department of Defense
DODI Department of Defense Instruction
DPC Data Protection Committee
DSG Data Sciences Group
EITDR Enterprise Information Technology Data Repository
eMASS enterprise Mission Assurance Support Service
FISMA Federal Information Security Management Act
GIG Global Information Grid
IA information assurance
IAC Information Assurance Control
IATO interim authorization to operate
IATT interim authorization to test
IG Inspector General
IT information technology
IV&V independent verification and validation
KS Knowledge Service
NIST National Institute of Standards and Technology
NMCI Navy/Marine Corps Internet
PIA Privacy Impact Assessment
PIT Platform IT
PMRF Pacific Missile Range Facility
POA&M Plan of Action and Milestones
RDDAA Research and Development Designated Accrediting Authority
RDT&E research, development, test, and evaluation
SECNAV Secretary of the Navy
SIP System Identification Profile
USAF United States Air Force
CHAPTER 1

INTRODUCTION

1.1 Survey

The Data Sciences Group (DSG) conducted a survey of Range Commanders Council (RCC) member ranges asking a series of key questions about common Information Assurance (IA) practices, identification of possible exemptions, and successful strategies and tools for tracking range IA programs. Ranges were also asked to provide notional "common" IA practices in a test mission environment to include a decision tree for interpretation and implementation of IA. Nine member ranges participated in the survey. The results from the survey are provided in Chapter 3 of this document.

1.2 Decision Tree

The Pacific Missile Range Facility (PMRF) uses an IA Applicability Matrix to determine IA requirements for various categories of Information Technology (IT), including PMRF-owned DIACAP assets, Platform IT (PIT), visiting systems, personally owned equipment, and foreign systems. The Applicability Matrix is, in effect, a decision tree for determining IA applicability and was provided to the DSG Data Protection Committee (DPC) during the March 2010 DSG meeting as a suggested decision tree for all ranges. The matrix is posted on the DPC site within the RCC Private Portal as a reference document for this task.
This page intentionally left blank.
CHAPTER 2
SURVEY AND BEST PRACTICES

The Data Protection Committee (DPC) conducted a survey of RCC members to query Information Assurance lessons learned and best practices. This chapter explains the survey methodology and presents the survey results.

2.1 Methodology

The survey was distributed to active DPC representatives. Responses were returned to the task lead and consolidated into lessons learned and best practices. The survey is posted on the RCC private website:

https://wsdmext.wsmr.army.mil/site/rccpri

2.2 Lessons Learned

Follow-on discussions at meetings of the Data Sciences Group (DSG) generated additional information. The following lessons learned were derived from survey responses, as well as comments made by DPC members.

2.2.1 IA Requirements.

a. DIACAP is often difficult to apply to specialized, real-time, closed networks, or prototype research, development, test, and evaluation (RDT&E) systems.

b. The Platform IT process is beneficial for ranges, as it offers more precise application of IA requirements and streamlined processes.

DPC members emphasized that Platform IT is not an excuse for avoiding implementation of IA or an attempt to “get out of” DIACAP, but rather it can be a very effective tool for more accurately focusing the application of IA requirements to specialized range systems.

c. Different interpretations exist among the Services in the application of Department of Defense Instruction (DODI) 8500.2, Information Assurance Implementation (6 Feb 03):
   (1) Organizations within each Service may not always have a clear understanding of their chain of command for accomplishing IA and Certification and Accreditation (C&A).
   (2) Confusion results from the Services using different names and titles to refer to similar job functions.

d. Full transition to DIACAP has not occurred at a few ranges.
e. Platform IT (PIT) designation and C&A processes are not uniformly understood or may not exist, therefore implementation varies among the Services.

f. The requirement to accredit RDT&E systems is not consistently understood by all stakeholders, yet DoD policy requires accreditation of these systems. The inconsistency leads to delivery of unaccredited systems, which creates issues for IA personnel attempting to apply mandated IA requirements.

g. There is a lack of IA training standards and courses for DIACAP and PIT processes and standards.

2.2.2 Process

a. Change of Certifying Authority (CA) and Designated Accrediting Authority (DAA) assignments contributes to lack of understanding of systems and disruption to the C&A process. Program managers would prefer to work with the same CA and DAA over time, if at all possible.

b. Lack of standard C&A tracking and DIACAP package creation tools contributes to variation in C&A packages and loss of the ability to monitor progress of the package as it transitions through the steps of the C&A process.

c. The C&A process is too lengthy and all Services noted completing the process and obtaining DAA approval is very resource intensive and time-consuming. Ranges often have short time line requirements that can be exceeded.

d. The use of a specialized CA and DAA (e.g., Navy Research and Development Designating Authority (RDAA)) can shorten approval times and increase efficiency of the process.

2.2.3 Resourcing

a. The RDT&E IT systems and networks can be old, making it difficult to apply more modern IA standards and practices. Updating old systems to comply with modern IA standards can be cost prohibitive or impossible.

b. Specialized RDT&E networks need to exist and many functions cannot be transitioned to Service Enterprise networks (e.g., Navy/Marine Corps Internet (NMCI)). For the Navy, this transition requires Cyber Asset Reduction and Security (CARS) designation of RDT&E networks as “Excepted Networks.”

c. Sufficient resourcing, such as money, time, and personnel, is mandated by DoD policy; however resourcing is almost always an issue. It was felt that leadership does not always support IA to the required level.

2.3 Best Practices

The following best practices are recognized by the DPC as minimal standards all practitioners of C&A should follow.
2.3.1 Common RCC Standards for IA/C&A.

b. Common IA Control interpretation and application.
e. Minimum C&A package contents:
   (1) System Description.
   (2) Accreditation Boundary.
   (3) Hardware and Software List.
   (4) External Connections.
   (5) List of applicable IA Controls and their implementation status (compliant, non-compliant, inherited, not applicable).
   (6) Test plan.
   (7) Test results supporting IA Control implementation status.
   (8) Risk Assessment.
   (9) Plan of Action and Milestones (POA&M) for resolving outstanding vulnerabilities.
f. Adopt a decision tree for determining IA applicability (see Chapter 3 and Reference 4.6b)

2.3.2 Platform IT (PIT).

a. Flexibility in the application of IA controls.
b. Streamlined process.

2.3.3 Designated Accrediting Authority (DAA) Issues.

a. Accreditation reciprocity.
b. Designate specialized, mission-oriented RDT&E DAA and CA authorities.
c. Implementation of baseline standards.

2.3.4 Training. Department of Defense Instruction 8570.1 (DODI 8570.1), Information Assurance Workforce Improvement Program, 20 April 2010, focuses on certain IA positions, but leaves out some IA-related positions (e.g., senior management, system owners, program managers, purchasing agents, engineering staff and others) and focus on top level processes.
This page intentionally left blank.
CHAPTER 3

DECISION TREE AND RECOMMENDATIONS

An example IA Applicability Matrix (Reference 4.6b was provided to the Data Protection Committee (DPC) in March 2010. The matrix was subsequently reviewed and accepted by the committee as a valid working document and is included as a recommended best practice.

3.1 Decision Tree

The IA Applicability Matrix provides a standardized method of determining which IA processes should be followed given various kinds of IT systems and networks, including:

a. Range owned IT subject to DIACAP.
b. Range owned IT designated as Platform IT.
c. DoD owned IT intended for permanent or temporary connection to range IT assets.
d. Stand-alone IT.
e. Commercially owned IT equipment.
f. Personally owned IT equipment.
g. Foreign government IT equipment.

3.2 Recommendations

The DPC recommends that the RCC:

a. Adopt the best practices listed in paragraph 2.3.
b. Issue a task to create an RCC IA standard based on implementation of the best practices listed in paragraph 2.3.
c. Direct the DSG to rename the Data Protection Committee to the Information Assurance Committee (IAC), which reflects the use of common lexicon within DoD.
This page intentionally left blank.
CHAPTER 4

REFERENCES

4.1 Federal


b. Section 11331 of title 40, United States Code.


http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=browse_usc&docid=Cite:+5USC552a.

4.2  DoD

http://www.dtic.mil/whs/directives/ or ASDNII.pubs@osd.mil.


http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNII.pubs@osd.mil.

http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNII.pubs@osd.mil.

http://www.dtic.mil/whs/directives/corres/html/85101m.htm or ASDNII.pubs@osd.mil.


   http://www.dtic.mil/whs/directives/ or USDI.Pubs@osd.mil.


s. DoD Instruction 8580.1, “Information Assurance (IA) in the Defense Acquisition System,” 9 Jul 2004. (Copies of this document are available online at 
   http://www.dtic.mil/whs/directives/corres/ins1.html or ASDNIIPubs@osd.mil.


   August 6, 1998. 

v. CJCSM 6510.01, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND),” 25 Mar 03. 

4.3 Navy


4.4 Air Force


4.5 Army

4.6 Range Specific

a. Pacific Missile Range Facility (PMRF) Platform IT (PIT) Template and DON PIT Questionnaire.

b. PMRF IA Applicability Matrix, dated April, 2010.

c. PMRF Compliance and Validation Certification (CVC) Guidebook, dated April, 2008.

4.7 Other: Web Links

a. The entire Secretary of the Navy (SECNAV) IA manual series may be accessed through the Department of Navy Issuances website: http://doni.daps.dla.mil.


c. PIAs must be conducted using the prescribed DON format located at http://www.doncio.navy.mil.


e. The Navy CDS Office (NCDSO), operated by SPAWAR, provides the Navy interface and representation to this DoD process. Specific guidance is provided on the NCDSO web page located at https://infosec.navy.mil/cds/cds_home.jsp.


4.8 Other: RCC References

a. DOCUMENT 172-08 - Data Sciences Group “DoD Information Assurance Certification and Accreditation Process (DIACAP): Impact Assessment.”

b. DIACAP Tiger Team Outbrief: Ryan Norman, JMETC Lead Systems Engineer, TRMC Lead for DIACAP Tiger Team, Ryan.Norman@osd.mil.

c. DIACAP Tiger Team Final Report, 11 June 2010.
This page intentionally left blank.
APPENDIX A

DIACAP BACKGROUND INFORMATION

1.1 DIACAP Process

The DIACAP contains the DoD processes for identifying, implementing, validating, certifying, and managing Information Assurance (IA) measures and services, expressed as Information Assurance Controls (IACs), and authorizing the operation of DoD IS in accordance with statutory, Federal and DoD requirements. The DIACAP is a comprehensive Certification and Accreditation (C&A) process that supports and complements the net-centric Global Information Grid (GIG)-based environment.

1.1.1 DIACAP Background

b. Replaces DITSCAP.
c. Process based on automated tools…but tools are not yet fully available.
d. Limited input fields and standardized databases - limit paperwork avalanche.
e. Attempts to further standardize test methods and “risk” categorization; remove subjectivity.
f. Severity Category Codes (I – III).
g. Impact Codes (High – Low).
h. Aligns C&A with FISMA Requirements.
i. Two associated Web-based services – the DIACAP Knowledge Service (KS) and the enterprise Mission Assurance Support Service (eMASS).
1.1.2 **DIACAP Knowledge Service (KS).**

a. Library of references, tools, diagrams, templates, process maps to aid in DIACAP execution.
b. Collaboration workspace for the DIACAP User Community.
c. Lessons learned and best practices.
d. [https://diacap.iaportal.navy.mil/login.htm](https://diacap.iaportal.navy.mil/login.htm)

1.1.3 **DIACAP Packages.**

a. **Executive Package.**
   (1) System Identification Profile (SIP).
   (2) DIACAP Scorecard.
   (3) Plan of Action and Milestones (POA&M), if required.

b. **Comprehensive Package.**
   (1) Executive Package (SIP, DIACAP Scorecard, POA&M)
   (2) DIACAP Implementation Plan
   (3) Supporting Documentation
      - “Artifacts”
      - Certification results
      - Materials required to support or justify compliance with all IA Controls

2.1 **DIACAP Activities**

A graphic of DIACAP activities is shown at Figure A-2.
The activity details, keyed to Figure A-2, are described below.

2.1.1 **Initiate and Plan C&A.**

a. **Register System.**
   (1) Army Portfolio Management System (APMS)
   (2) Navy Information Assurance Tracking System (IATS)
   (3) Create System Identification Profile (SIP)

b. **Assign IA Controls.**
   (1) Baseline Controls plus Service and system unique IA Controls

c. **Assemble DIACAP Team.**

d. **Create DIACAP Implementation Plan.**
   (1) Assign Responsibilities
   (2) Allocate Resources and Schedule

2.1.2 **Implement and Validate IA Controls.**

a. **Execute DIACAP Implementation Plan.**
   (1) Implement the IA Controls

b. **Conduct Validation Activities.**
   (1) DITSCAP Lite?

c. **Compile Validation Results using DIACAP Scorecard.**
   (1) Risk Assessment Lite?

d. **DIACAP Scorecard.**
   (1) Summary of system IA Control compliance status (compliant, non-compliant, N/A)
   (2) Intended to convey information about the IA posture of the evaluated system in a format that can be easily understood by managers.
   (3) Rigid definitions for Probability of Exploitation and Degree of Impact (Harm)
      - Severity Code
      - Impact Code
   (4) Severity Category
      - I  – Allows security to be by-passed, resulting in immediate unauthorized or root-level access
      - II – Potential to lead to unauthorized access
      - III – Recommendations that will improve IA posture
   (5) Impact Code
      - High  – “Severely Disrupt” GIG
      - Medium – “Moderately Disrupt” GIG
      - Low  – “Minimally Disrupt” GIG
2.1.3 Make Certification Determination and Accreditation Decision.

a. Make Certification Determination.
   (1) Severity Code.
   (2) Impact Code.

b. Issue Accreditation Decision.
   (1) Danger to the Global Information Grid (GIG): interim authorization to test (IATT), interim authorization to operate (IATO), authorization to operate (ATO), and denial of authorization to operate (DATO).

1. Single CA for each Service determines risk.

2. Only the Service Chief Information Officer (CIO) can authorize operation for a system with a Severity Category I finding.

NOTE

2.1.4 Maintain Authorization and Conduct Reviews (Comply with FISMA).

a. Maintain situational awareness.

b. Annual revalidation of some IA controls.

c. Must result in 100 PERCENT review of all IA controls over 3-year period.

d. Maintain IA posture.

e. Annual status report with recommendations.

f. A designated accrediting authority (DAA) decision to continue/alter prior approval.

2.1.5 Decommission.

a. Address disposition of DIACAP registration information.

b. Address disposition of system-related data or objects in GIG.
3.1 Service DIACAP Methodologies

The current DIACAP methodologies used by RCC member Services are described in the following subparagraphs.

3.1.1 Air Force.

a. Enterprise Information Technology Data Repository (EITDR). The EITDR is a database controlled and managed by AFCA and used as a repository for FISMA compliance that includes information on most unclassified United States Air Force (USAF) IT systems. All data is uploaded from the EITDR into the DoD Information Technology Profile Registry (DITPR) to meet Federal Information System Management Act (FISMA) requirements. Information from DIACAP is only a small part of the data collected in the EITDR. The system is used to keep track of new acquisitions, new major DoD mandate compliance, program management, and system engineering documentation. The program manager is responsible for validation and the Certifying Authority (CA) is responsible for certification.

The EITDR allows stakeholders to set milestones and put the system through each phase of the DIACAP process. It also allows the producer to automatically create POA&Ms, System Identification Profile (SIP), DIACAP Implementation Plan (DIP), and DIACAP Scorecard.

b. DIACAP Knowledge Service Templates. In addition to EITDR, some USAF systems use the DIACAP Knowledge Service templates to accomplish the C&A process.

3.1.2 Army. The Army follows Army Regulation 25-2, Information Management-Information Assurance. The Army Portfolio Management Solution (APMS) is the Army’s system and it has four major modules:

a. IT registration module.
b. Domain Certification module.
c. Capital Planning and Investment Management IT Prioritization Module.
d. Capital Planning Investment Control IT Budget Reporting Module.

All the databases do essentially the same thing. For the purpose of DIACAP, the IT registration and IA certification components are the most important. Figure A-3 depicts the Army accreditation process.
3.1.3  **Navy.** The Navy implements DIACAP by using DoD Instruction 8510.01 (Reference 4.2b). A flowchart/decision tree known as PMRF IA Applicability Matrix, April, 2010 (Reference 4.6b is posted on the Data Protection Committee’s site on the RCC Private Portal.

The DIACAP is the overarching C&A process for the DoD. The DON DIACAP Handbook, V1.0, 15 July 2008 (Reference 4d provides the overarching guidance of the DON’s implementation of DIACAP. The Navy provides Service-unique amplification to successfully execute these processes while maintaining the intent of DIACAP as set forth in this handbook.

a. **C&A Documentation.** DIACAP uses a data-driven approach as much as practical for C&A documentation. To standardize the way C&A activities are documented, a series of templates for entering data has been created. The DIACAP templates and examples can be found at: https://www.portal.navy.mil/netwarcom/navycanda/default.aspx

b. **Department of Navy (DON) DIACAP Activities.** The DON follows the DoD activities which are summarized in Figure A-4.

3.1.4  **Marine Corps and Coast Guard.** There were no Marine Corps or Coast Guard ranges participating in the survey or on the Data Protection Committee.
3.1.4 Marine Corps and Coast Guard. There were no Marine Corps or Coast Guard ranges participating in the survey or on the Data Protection Committee.

**** END OF DOCUMENT ****