DATA ITEM DESCRIPTION

Title: Information Assurance (IA) Test Report

Number: DI-MGMT-81843
AMSC Number: N9220
DTIC Applicable: N/A
Office of Primary Responsibility: SH/PEO IWS 1.0
Applicable Forms: N/A

Approval Date: 20111108
Limitation: N/A
GIPDEP Applicable: N/A

Use/Relationship: The IA Test Report will be used by the government to manage Information Assurance testing that will result in accreditation of the ship based information technology system to comply with Information Assurance policies and criteria.

This Data Item Description (DID) contains the format and content preparation instructions for the data resulting from the work task specified in the contract.

Requirements:

1.0 Format. The IA Test Report shall be presented in the contractor's format.

2.0 Content. The report shall address the following sections:

a. Introduction
b. System Nomenclature
c. Purpose of the test
d. A description of the system/subsystem being tested.
e. Threat Model for System Under Test
   (1) Internal and External IA Threat Exploits
   (2) Mitigations by Design, Inheritance or Procedure
f. Security Testing Boundary Diagram
g. Bill of Materials for Security Testing Boundary
h. Indicated Network topology with Test Points
i. Master Network Connection Report (MNCR) for Security Testing Boundary
j. Identify the applicable DISA approved Test Tools
k. Assumptions regarding test procedures, test conditions and test environment

l. Test Point Matrix which shall identify:
   (1) Machine under test
   (2) DISA Approved Test Tool
   (3) If Test Tool is installed on machine under test
   (4) A justification for chosen Test Point and Test Tool

m. Personnel Responsibility Matrix shall identify names, official job titles, and functions and responsibilities.

n. Security Test Resource shall specify:
   (1) Required Materiel
   (2) Materiel Provider
   (3) Materiel Due Date
   (4) Readiness Status

o. Security Testing Schedule shall include:
   (1) Location
   (2) Test Event Activity:
      (a) In-Brief to Site Lead
      (b) Execute Test
      (c) Out-Brief to Site Lead
      (d) Secure Assets and Materials
   (4) Start and End Dates
   (5) Lead Person for Test Event Activity

p. Security Test Procedures shall include:
   (1) The risks and threat levels of the existing security implementations
   (2) Deviations from the IA Test Plan with Rationale
   (3) Network discovery procedures via automated tools
   (4) Operating System discovery procedures via automated tools
   (5) Discovering ports, protocols and services via automated tools
   (6) Vulnerability scan via automated tools
   (7) Host Based Testing
   (8) Application Testing
   (9) Testing done manually in accordance with the applicable Security Technical Implementation Guide (STIG) used.

q. Justification for any false positives and the following:

(1) Finding Tracking Number
(2) Configuration Name and Nomenclature
(3) Affected Internet Protocol Address
(4) Network Node Name
(5) Title of STIG Reference including STIG Version
(6) STIG Reference Paragraph
(7) Applicable IA Controls specified in DoDI 8500.2
(8) Vulnerability Findings
(9) Rationale why compliance is not met
(10) Severity Risk Rating (Cat I, II, III)
(11) Consequence or Impact of vulnerability
(12) Recommendation for correcting the findings
(13) Engineering Response
(14) Estimated Completion Date
(15) Status of Fix Verification

3.0 Media Requirement. The electronic media for the IA test report shall be Microsoft Office Word Version 2003-2007.

4.0 End of DI-MGMT-81843. .

DI-MGMT-81843
Figure 1

Finding Tracking Number	Configuration Name and Nomenclature	Affected Internet Protocol Address	Network Name	Finding or Vulnerability	Consequence or Impact	Risk Rating	Recommendations	Engineering Response	Estimated Completion Date	Status of Fix Verification	Comments

Information Assurance Findings Matrix