DATA ITEM DESCRIPTION

Title: Information Assurance (IA) Design Review Information Package (DRIP)

Number: DI-MGMT-81845
AMSC Number: N9222
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 Information Assurance (IA) Design Review Information Package (DRIP) will be used by the government to review the Defense in-Depth (DiD) design and support the Platform Risk Assessment (PRA) of the ship.

This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement delineated in the contract.

Requirements:

1.0 Format. The IA DRIP shall be presented in format similar to that of Figures 1 through 7.

2.0 Content. The IA DRIP workbook shall contain updatable tables for the each section.

2.1 Executive Summary, Section 1. This section shall contain all of the information specified in figure 1 and shall also identify following:

a. System description and purpose.
b. Mission Assurance Category per DoDI 8500.2
c. Security Classification.
d. Security Mode of Operation.

2.2 Information Assurance Certification and Accreditation (IA C&A) Boundary, Section 2. This section shall be presented in a format similar to that of Figure 2 and shall contain the following headings:

a. Schematic Interface Diagram placed above the headings showing:
   (1) Major Subsystems
   (2) Information Assurance defense points including:
      (a) Firewalls
      (b) Routers
b. Nomenclature name of each subsystem within IA C&A Boundary
c. Functional description of each subsystem within IA C&A Boundary
d. Description of User Roles and Privileges of each subsystem within IA C&A Boundary
e. Technical Cyber Defense Mitigation in each subsystem within IA C&A Boundary

e. Critical Protected Information (CPI) of each subsystem within IA C&A Boundary (CPI provided as a classified attachment)

2.3 System Requirements Verification Matrix (IA SRVM), Section 3. This section shall be presented in a format similar to that of Figure 3 and shall also contain the following headings:

a. Applicable DoDI 8500.2 IA Controls
b. Software Requirement Specifications (SRS)
c. System Subsystem Specifications (SSS) to illustrate how the Defense in-Depth (DiD) design meets the IA Controls.

2.4 The IA MNC section shall be presented in a format similar to that of Figure 4 and shall also contain the following headings:

a. Date of data entry into the MNC
b. Description of function provided by or supported by connection
c. Reference Application Programming Interface (API) specification
d. LAN Technology
e. IP of the Data Source device transmitting data
f. Subnet Mask
g. Default Gateway
h. Hostname of the Data Source device transmitting data
i. Classification of the Data Source device transmitting the data
j. Classification of the actual data being transmitted
k. Network Data Transfer Protocol used to transmit the data
l. Data Delivery Type: Bi-Directional, Uni-Directional or Multicast
m. IANA Port Number assigned to transmit the data
n. Service daemon transmitting the data
o. Is Port, Protocol and Service approved by DISA (Yes or No)
p. Data encryption standard used
q. Is Data Source device inside the IA C&A Boundary (Yes or No)
r. IP of the Data Sink/Destination device receiving transmitted data
s. Hostname of the Data Sink/Destination device receiving data
t. Classification of the Data Sink/Destination device receiving data
u. Is Data Sink/Destination device within IA C&A Boundary (Yes or No)

2.4.1 The Information Assurance-Master Network Connection (IA MNC), Section 4. This section shall contain the basis for building Access Control Lists (ACLs) in accordance with the following DODI 8500.2 IA Controls:

(a) DCPP-1 Ports, Protocols, and Services

(b) DCFA-1 Functional Architecture for AIS Applications,
(c) DCFA-1 Functional Architecture for AIS Applications,
(d) DCID-1 Interconnection Documentation and
(e) ECIC-1 Interconnections Among DoD Systems and Enclaves.

2.4.2 The IA-MNC section shall identify changes when made to the network connections in system upgrades or Engineering Change Proposals (ECPs).

2.4.3 The IA-MNC section shall identify all network connections that route to, from, through and across the networked subsystems within the Information Assurance Certification and Accreditation (IA C&A) boundary.

2.4.4 The IA-MNC section shall specify the network connections for capabilities and functions performed within the Information Assurance boundary "the enclave".

2.5 Common Assurance System Architecture (CASA) Section 5. This section shall be presented in format similar to that of Figure 5 and shall contain the following headings:

a. Incident Alert Categories
b. Incident Alert Conditions

2.6 Threat Model for IA C&A Boundary, Section 6. This section shall be in presented in format similar to that of Figure 6 and shall contain:

a. Internal and External IA Threat Exploits
b. Technical and Logical Mitigations
c. Mitigation by Design, Inheritance or Procedure

2.7 Applicable STIGS for IA C&A Boundary, Section 7. This section shall be in presented in format similar to that of Figure 7 and shall contain:

a. Applicable STIG
b. Rationale

3.0 Media Requirement. The electronic media for the IA DRIP package shall be Microsoft Excel, Version 2003-2007.

4.0 End of DI-MGMT-81845.

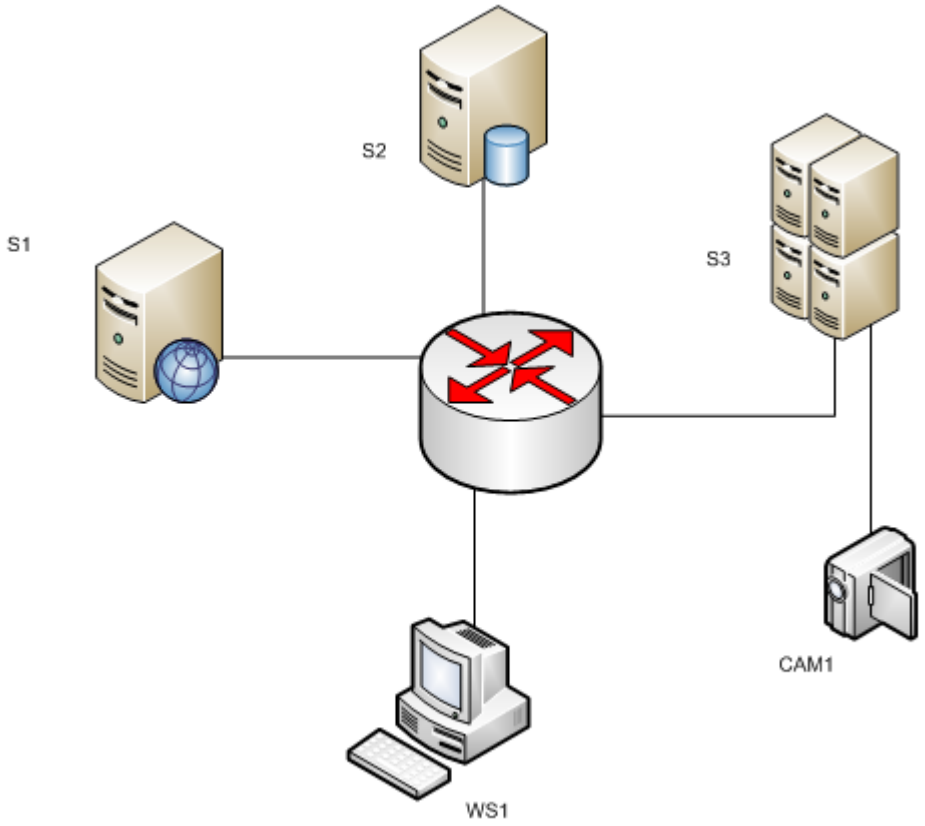
DI-MGMT-81845

Figure 1

Executive Summary

Design Review Information Package

System Nomenclature	System description and purpose	Mission Assurance Category per DoDI 8500.2	Security Classification	Security Mode of Operation



Information Assurance Certification and Accreditation (IA C&A) Boundary

Schematic Node ID	Nomenclature of subsystem	Functional Description of subsystem	Description of User Roles and Privileges on subsystem	Description of Technical Mitigations in subsystem	Critical Protected Information (CPI) SEPARATE CLASSIFIED ATTACHMENT

Information Assurance (IA) System Requirements Verification Matrix (SRVM)

Applicable DoDI 8500.2 IA Controls	Software Requirement Specifications (SRS)	System Subsystem Specifications (SSS)

DI-MGMT-81845

Figure 4

INFORMATION ASSURANCE MASTER NETWORK CONNECTION REPORT (IA-MNCR)

Date of Data Entry to the MNCR	Description of Function	Reference API Specification	LAN Technology	IP of the Data Source	Subnet Mask	Default Gateway	Host Name	Classification of Data Source	Classification of Actual Data being Transmitted	Network Data Transfer Protocol Used to Transmit the Data	Data Delivery Type: Bi or Uni Directional or Multicast	IANA Port Number Assigned to Transmit Data	Service Daemon Transmitting the Data	Is Port, Protocol and Service approved by DISA (Y/N)

Data Encryption Standard used	Is Data Source Device Inside the IA C&A Boundary (Y/N)	IP of the Data Sink/ Description Device Receiving Transmitted Data	Hostname of the Data Sink/ Destination Device Receiving Data	Classification of the Data Sink/ Destination Device Receiving Data	Is Data Sink/ Destination Device within IA C&A Boundary (Y/N)

Figure 5

Common Assurance System Architecture (CASA)

Incident Alert Category	Incident Alert Condition

Figure 6

Threat Model

Threat Exploit	Threat Mitigation Description	Mitigation by Design, Inheritance or Procedure

Figure 7

Applicable STIGS

STIG Title	Rationale