DATA ITEM DESCRIPTION

Title: Vulnerability Scan Compliance (VSC) Report

Number: DI-MGMT-81842
AMSC Number: N9219
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 VSC Report will be used by the government to assess the security vulnerability and residual risks of a major information system software build.

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

The reference document cited in this DID can be obtained from http://iase.disa.mil/stigs/index.html

Requirements:

1.0 Reference: The applicable issue of documents cited herein, including their approval dates and dates of any applicable amendments, notices and revisions, shall be as reflected in the contract.

2.0 Format. The VSC Report shall be presented in Microsoft Office Excel spreadsheet format similar to that of Figure 1.

3.0 Content. The VSC Report shall contain the following headings:

(a) Title of Security Technical Implementation Guide (STIG) Reference including STIG Version
(b) STIG Reference Paragraph
(c) Applicable IA Controls from DoDI 8500.2
(d) Severity Risk Rating (Cat I, II, III)
(e) Compliance Status shall be specified as one of the following:
  (1) Yes
  (2) No
(f) Compliance Rationale
  (1) identify design implementation to satisfy compliance
  (2) identify procedures taken to satisfy compliance
  (3) identify document used to satisfy compliance
  (4) identify why compliance is not met and the consequence of non-compliance

(g) System Impact (for non-compliant items only)
  (1) identify impact to capability to execute mission
  (2) identify risk exposure to threat
(h) Mitigation Recommendations (for non-compliant items only)

3.1. The VSC Report shall identify all open findings with recommendations on how the findings will be mitigated based on the approved applicable DISA STIGs and shall include the following:

a. Application Security and Development STIG
b. Access Control STIG
c. Application Services STIG
d. Database STIG
e. Desktop Application STIG
f. Defense Switched Network (DSN) STIG
g. Directory Services STIG
h. DISA Instruction Enclave STIG
i. Domain Name System (DNS) STIG
j. Enclave STIG
k. ERP STIG
l. ESM STIG
m. ESX Server STIG
n. Instant Messaging STIG
o. Network STIG
p. Personal Computer Communications Client (Voice-Video-Collaboration) STIG
q. Sharing Peripherals Across the Network (SPAN) STIG
r. Secure Remote Computing STIG
s. UNIX STIG
t. Virtual Machine STIG
u. Voice Over Internet Protocol (VOIP) STIG
v. Web Server STIG
w. NSA Windows NT Guide
x. NSA Windows 2000 Guides
y. Windows 2000/XP/2003/Vista Addendum

4.0 Media Requirements: The electronic media for the VSC Report shall be Microsoft Excel Version 2003-2007.

5.0 End of DI-MGMT-81842.

Figure 1

Title of STIG Reference including STIG Version	STIG Reference Paragraph	Applicable IA Controls from DoDI 8500.2	Severity Risk Rating (Cat I, II, III)	Compliance Status	Compliance Rationale	System Impact	Mitigation Recommendation

VULNERABILITY SCAN COMPLIANCE (VSC) REPORT