DATA ITEM DESCRIPTION

Title: System Security Administrator Operators Documentation (SSAOD)

Number: DI-MGMT-81857
AMSC Number: N9239
DTIC Applicable: N/A
Office of Primary Responsibility: SH/PEO IWS1.0
Applicable Forms: N/A

Approval Date: 20111221
Limitation: N/A
GIPDEP Applicable: N/A

Use/Relationship: The SSAOD developed by the contractor will be integrated into a baseline OPSEC training manual by the government to train the audit and archive procedures and the operation of the anti-cyber warfare capabilities provided in the delivered system.

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

Requirements:

1.0 Format. The System Security Administrator Operators Documentation shall be presented in a format similar to that of Figures 1 and 2.

2.0 Content. The System Security Administrator Operators Documentation shall contain Appendixes "A" through "E".

2.1 Appendix A shall identify:
- a. Clearing IA Alarms
- b. Appendix A.2 shall identify Diagnosing IA Alarms
- c. Appendix A.3 shall identify Generating an Incident Report Summary

2.2 Appendix "B" shall include Changing Passwords:
- a. Appendix B.1 shall identify changing passwords on workstation consoles
- b. Appendix B.2 shall identify changing password procedures for rack mounted cpus
- c. Appendix B.3 shall identify changing password procedures for the automated status board
- d. Appendix B.6 shall identify changing password procedures for network devices
- e. Appendix B.7 shall identify changing file integrity checker passphrases
- f. Appendix B.8 shall identify changing file integrity checker passphrase
- g. Appendix B.9 shall identify changing audit tool password
- h. Appendix B.9.1 shall identify changing audit tool password for security administrator
- i. Appendix B.9.1 shall identify changing audit tool password for system administrator

2.3 Appendix "C" shall be entitled Conduct System Audit. This appendix shall specify procedures to identify system misuse and hacker threat attacks. It shall detail what action should be taken if a security violation is found. This appendix shall also include the procedures to identify the following auditable items from the contractor's delivered system:

a. List of Hostnames Included in the audit report
b. List of Hostnames not Included in the audit report
c. Alphabetical list of authorized usernames
d. Chronological list of successful login attempts organized by Information System (IS)
e. Chronological list of failed login attempts organized by IS
f. Chronological list of successful sulog attempts organized by IS
g. Chronological list of failed sulog attempts organized by IS
h. Chronological list of alerts from the Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) organized by IS
i. Chronological list of file monitor alerts organized by IS
j. Chronological list of system status
k. Chronological list of successful root login attempts organized by IS
l. Chronological list of root login attempts organized by IS
m. Chronological list of user additions or deletions organized by IS
n. Chronological list of password change attempts, both successful and unsuccessful organized by IS
o. Chronological list of router/switch login attempts, both successful and unsuccessful organized by IS
p. Chronological list of enable router/switch login, both successful and unsuccessful organized by IS

2.4 Appendix "D" shall be entitled "Archive Security Logs". This appendix shall provide procedures to archive audit logs to removable backup media that will be stowed in a GSA-approved security container. This appendix shall include warnings to users that security audit logs and reports shall be kept for one year. This appendix shall also include warnings to users hat record destruction shall be specified.

2.5 Appendix "E" shall include procedures generating the Formal Incident Report. This appendix shall provide the procedures for reporting and documenting a computer security incident on DoD computer equipment to the Navy Cyber Defense Operations Command (NCDOC), the In-Service Engineering Agent, Program office and its support activities. This appendix shall include the procedures for crew submittal of an OPREP3. This appendix shall also specify the procedures to be used for reporting incident details after the OPREP-3 is sent.

3.0 Media Requirements: The SSAOA electronic media shall be Microsoft Word Version 2003-2007.

4.0 End of DI-MGMT-81857.

- Figure 1 -

HOW TO USE THIS APPENDIX

This appendix uses different text styles to assist you in understanding the content as follows.

DEFINITIONS

Items throughout this appendix which have definitions will be shown as the following:

Confidentiality

Availability

NOTE BOXES

A Note box like the one shown below is used to provide additional information.

NOTE	**Conveys information or an example that amplifies or illustrates the subject that was just presented.**

WARNING BOXES

A Warning box like the one below is used to provide consequences if the procedures are violated. Consequences may lead to disciplinary action or loss of life.

WARNING	**Conveys consequences for not following the regulations and procedures. Consequences may lead to loss of life or criminal prosecution.**

CHOOSING GRAPHICAL USER INTERFACE MENU ITEMS

This appendix may provide procedures that require input by pointing and clicking on the graphical user interface (GUI). A GUI with a drop down menu that must be selected or a GUI button that must be clicked will be described using the following text style:

"Open"

"OK"

SYSTEM ACCOUNTS

Throughout this appendix the use of system accounts will be shown in italicized text as follows:

Root

SysAdm

PRESSING THE RETURN OR ENTER KEY

This appendix may provide procedures that require keyboard input by pressing the carriage return or by pressing the "Enter" key. The "Enter" key will be represented in this appendix as:

<enter>

TYPING EXACTLY AS SHOWN

This appendix may provide procedures that require keyboard input by typing in text exactly as shown in this appendix. Such text will be represented in this appendix as:

ii=/usr/local/etc/ssh_known_hosts <enter>

NOTE	The "Enter" key is pressed in the above example.

TYPING VALUE WHEN THE INFORMATION VARIES

This appendix may provide procedures that require keyboard input by typing in text not explicitly provided in this appendix or the exact text may be in a reference. When text must be substituted, a placeholder will be represented in this appendix as:

***<password>*<enter>**

- Figure 2 -

APPENDIX B.1 CHANGE PASSWORDS ON WORKSTATION CONSOLES

Quick Reference Guide:	How to change passwords.
Purpose:	Maintenance procedures to periodically change the password to ensure the system uses secure and uncompromised passwords.
Description:	This appendix provides the procedure for changing passwords on the Host Based Intrusion Detection System.

1. From the System Administration drop down list, select "Password Administration" as shown in Figure xx.

Place Actual Screen Capture Here

Figure xx: System Administration Drop Down Menu

2. Once you select the "Password Administration" button, you will be prompted to enter the current password.

NOTE	**The current password is the initial password setup per the instructions in the Software Version Document (SVD).**

3. Enter the ***<current password>*** and click "OK".