

Scorecard Report

Generated on 08-May-2006 at 17:02.

CTS - Clean Test System

Description:

Type: AIS Application

C & A Status: Authorization to Operate (ATO)

System Classification: Confidential - FOR DEMO PURPOSES ONLY

Package Classification: Confidential - FOR DEMO PURPOSES ONLY

System Category:

System Owner: Department of Defense

System Sponsor: Department of Defense

Revalidation Date: 01-May-2007

CC Mission Category: Does Not Apply

System Artifacts: Yes

Mission Area
<u>Primary:</u> Business
<u>Secondary:</u> N/A
<u>Tertiary:</u> N/A
<u>Domain:</u> N/A

IT Registry
<u>Primary:</u> N/A
<u>Secondary:</u> N/A
<u>Tertiary:</u> N/A
<u>System ID:</u>

System Comments:

Control Icon Key

Mandated: 

Upgraded: 

Added: 

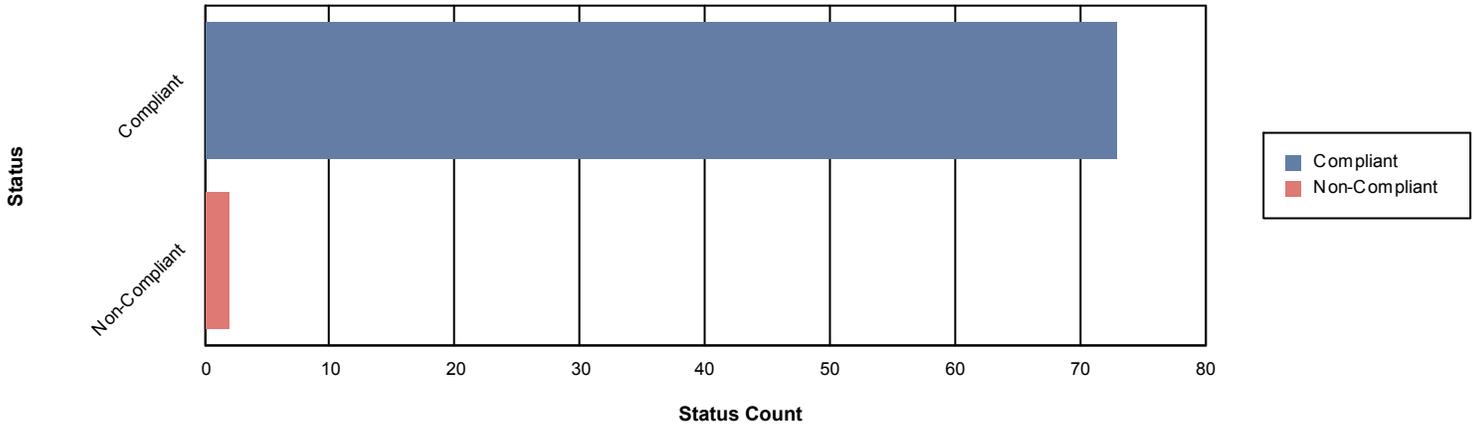
Inherited: 

Self Assessment: 

Scorecard Report

Generated on 08-May-2006 at 17:02.

System Compliance



	Compliant	Non-Compliant	Total
DoD Confidentiality: Classified, Public, Sensitive	5	0	5
DoD Confidentiality: Public	3	0	3
DoD Confidentiality: Public, Sensitive	3	0	3
DoD Confidentiality: Public, Sensitive MAC: 3	1	0	1
MAC: 1, 2, 3	38	0	38
MAC: 2, 3	4	0	4
MAC: 3	19	2	21
DoDI 8500.2	73	2	75
Total	73	2	75

Control Icon Key

Mandated: M

Upgraded: U

Added: A

Inherited: I

Self Assessment: SA

Scorecard Report

Generated on 08-May-2006 at 17:02.

Guidance Authority: DoDI 8500.2 Control Set

Selection Criteria: MAC: 3
DoD Confidentiality: Public

Status Summary: **Compliant: 73** **Non-Compliant: 2** **Not Tested: 0** **N/A: 0** **Total: 75**

Subject Area: Continuity (CO)

M COAS-1 Alternate Site Designation *Impact: High*

Control Status: **Compliant**

POA&Ms Exist: **Yes**

Validation Test : COAS-1-1

Validation Test Status: **Compliant**

System Name

Clean Test System

Status

Compliant

Comments

Validated: Actual alternate site has been identified in the COOP. Please see SSAA Appendices.

Validation Test : COAS-1-2

Validation Test Status: **Compliant**

System Name

Clean Test System

Status

Compliant

Comments

Validated: A comprehensive and effective COOP is in place to ensure implementation of continuity of mission or business-essential functions over a broad spectrum of emergency situations.

Validation Test : COAS-1-3

Validation Test Status: **Compliant**

System Name

Clean Test System

Status

Compliant

Comments

Validated: The COOP program includes a strategy for recovery and mission or business-essential operations system operations at the alternate site for an extended period of time.

Validation Test : COAS-1-4

Validation Test Status: **Compliant**

System Name

Clean Test System

Status

Compliant

Comments

Validated: Restoration of mission or business-essential system functions have been based on business impact analyses that describe and rank mission-critical applications and resources. System documentation lists maximum allowable outage times for these resources.

Validation Test : COAS-1-5

Validation Test Status: **Compliant**

System Name

Clean Test System

Status

Compliant

Comments

Validated: A contingency plan exists that identifies mission-essential computing needs to include hardware, software, communication lines, applications, and data. Verify that plan includes the operators, management, and technical support personnel that will implement the plan.

M COBR-1 Protection of Backup and Restoration Assets *Impact: High*

Control Status: **Compliant**

POA&Ms Exist: **No**

Validation Test : COBR-1-1

Validation Test Status: **Compliant**

System Name

Status

Comments

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Clean Test System	Compliant	Validated: Appendix L Section 12 Paragraph f: • Develop site access and security procedures for personnel relocating to their facilities. The procedures should anticipate the potential needs of relocated personnel (such as for keys and access codes to the sites) during both duty and non-duty hours. • Ensure that sufficient office space is designated to support the Director, Principal Deputy Director, Deputy Director, and Crisis Response Cell. • Provide storage space for classified documents and media. • Provide computers and network access (e.g., SIPRNET, CTS LAN). • Provide secure voice communication equipment X. • Ensure relocations sites have non-secure telephone and FAX capabilities. In addition, at least one outside line at each site much work independently from the telephone switch system (i.e., direct dial phone) in case of power outages.
M	CODB-1 Data Backup Procedures <i>Impact: Moderate</i>	POA&Ms Exist: No
Control Status: Compliant		
Validation Test : CODB-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Appendix L Section 4: • Maintain daily, weekly, and monthly backups for all X managed common servers within CTS. These backups will be restored to shared folders on servers within the relocation sites. Self-Assessment Alex 06-Apr-2006 Saify, Alex 06-Apr-2006 Compliant Also Appendix K 2.4: In many instances, the only way to recover from an incident is to restore systems from backup. Each CTS component is responsible to backup their respective systems in accordance with local policies. At a minimum, information on the servers and other mission critical systems should be backed-up nightly with a full backup at least weekly. A full system recovery from backup should be tested at least annually. Backup media should be stored off-site for at least 1 year and maintained in accordance with DISA policy. All compromised systems should also be backed up prior to restoring them to their original configuration. This backup of the compromised systems will be useful in the after actions and evidence gathering stages of incident handling.
M	CODP-1 Disaster and Recovery Planning <i>Impact: Moderate</i>	POA&Ms Exist: No
Control Status: Compliant		
Validation Test : CODP-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Reviewed: A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation.
M	COEB-1 Enclave Boundary Defense <i>Impact: High</i>	POA&Ms Exist: No
Control Status: Compliant		
Validation Test : COEB-1-1		

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: See Appendix L: Sections 11 and 12
M COED-1 Scheduled Exercises and Drills <i>Impact: Moderate</i>	Control Status: Compliant POA&Ms Exist: No	
<u>Validation Test : COED-1-1</u>		
<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: Yes, according to SSAA section 1.3.2, COOP plan is tested annually.
M COEF-1 Identification of Essential Functions <i>Impact: Moderate</i>	Control Status: Compliant POA&Ms Exist: No	
<u>Validation Test : COEF-1-1</u>		
<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: Business functionality has been identified in the Continuity of Operations Plan
M COMS-1 Maintenance Support <i>Impact: Moderate</i>	Control Status: Non-Compliant POA&Ms Exist: Yes	
<u>Validation Test : COMS-1-1</u>		
<u>Validation Test Status:</u> Non-Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Non-Compliant	Validated: Non compliant. While maintenance staff are mentioned in the Appendices, there is no mention of actual response time.
M COPS-1 Power Supply <i>Impact: Moderate</i>	Control Status: Compliant POA&Ms Exist: Yes	
<u>Validation Test : COPS-1-1</u>		
<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: Manually activated emergency power generators can restore electrical power. This is met by building regulations.
M COSP-1 Spares and Parts <i>Impact: Moderate</i>	Control Status: Compliant POA&Ms Exist: No	
<u>Validation Test : COSP-1-1</u>		
<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Not Applicable	System criticality does not warrant 24/7 uptime
M COSW-1 Backup Copies of Critical SW <i>Impact: High</i>	Control Status: Compliant POA&Ms Exist: No	
<u>Validation Test : COSW-1-1</u>		
<u>Validation Test Status:</u> Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Compliant, according to SSAA section 1.3.2 and COOP
M COTR-1 Trusted Recovery <i>Impact: High</i>	Control Status: Compliant POA&Ms Exist: No	
<u>Validation Test : COTR-1-1</u>		

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	1) System documentation includes detailed information on secure system recovery. 2) Mitigating circumstances and alternate locations have been documented extensively

Subject Area: Enclave Boundary Defense (EB)

M	EBBD-1 Boundary Defense <i>Impact: High</i>	
	Control Status: Compliant	POA&Ms Exist: No
Validation Test : EBBD-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Firewalls are deployed at the enclave boundary, as well as within the enclave to protect from internal compromise. NIDS sensors are deployed throughout the enclave, and are managed by a central IDS controller. All network access is through the DMZ and over NIPRNET

M	EBCR-1 Connection Rules <i>Impact: Moderate</i>	
	Control Status: Compliant	POA&Ms Exist: No
Validation Test : EBCR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: There is currently no MOA for connections to external DoD enclaves, as there is no necessity to connect to external resources.

M	EBPW-1 Public WAN Connection <i>Impact: High</i>	
	Control Status: Compliant	POA&Ms Exist: No
Validation Test : EBPW-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All NIPRNET traffic is connected through a DMZ. See Appendix I for thorough diagrams and documentation.

M	EBVC-1 VPN Controls <i>Impact: Moderate</i>	
	Control Status: Compliant	POA&Ms Exist: No
Validation Test : EBVC-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: NIDS sensors and controllers can capture and aggregate all network traffic data. Currently, only registered VPN traffic has been recorded over the network.

Subject Area: Enclave Computing Environment (EC)

M	ECAR-1 Audit Record Content – Public Systems <i>Impact: High</i>	
	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECAR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Audit logs reflect required information and are maintained in accordance with DoD policy for 180 days.

M	ECAT-1 Audit Trail, Monitoring, Analysis and Reporting <i>Impact: Moderate</i>	
Control Icon Key Mandated: M Upgraded: U Added: A Inherited: I Self Assessment: SA		

Scorecard Report

Generated on 08-May-2006 at 17:02.

Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECAT-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Firewall audit logs record all DoD required data and are stored offsite for 180 days.
M	ECED-1 Changes to Data <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECED-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Access controls are in place at all points of ingress/egress. In addition, all terminals implement strict user login and password policies, and all user activity for any given system is logged.
M	ECIM-1 Instant Messaging <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECIM-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Instant Message traffic, together with any and all unapproved IP traffic is blocked throughout the enclave. See Appendix I Section 12.
M	ECLP-1 Least Privilege <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECLP-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Access procedures enforce the concept of least privilege as it is applied to all system users. See Appendix I, Section 28 for complete details.
Validation Test : ECLP-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Both privileged and non-privileged accounts exist for specified system users.
M	ECMT-1 Conformance Monitoring and Testing <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECMT-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: IA monitoring and penetration testing has been documented in the Requirements Traceability Matrix, item number 20
M	ECND-1 Network Device Controls <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECND-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Clean Test System	Compliant	Validated: IAVA solutions are applied as necessary, with turnaround depending on their level of severity. Please see Appendix FF for a complete list of IAVAs that have been applied to the CTS.
M ECPA-1 Privileged Account Control <i>Impact: High</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECPA-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All accounts are granted roles based on "least privilege" access schemes. See Appendix I, sections 10-12
M ECPC-1 Production Code Change Controls <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECPC-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All code is managed using a CVS tree. Any changes to code must be approved by the CCB before being implemented by developers.
M ECRG-1 Audit Reduction and Report Generation <i>Impact: Basic</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECRG-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Audit logs can be viewed/analyzed by means of various software interfaces, to include NIDS controller, Firewalls, and OS tools.
M ECRR-1 Audit Record Retention <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECRR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Audit trails are maintained for one year. Regularly scheduled audit log backups are completed on a weekly basis for operating systems. All backups are stored offsite, in a fireproof container.
M ECSC-1 Security Configuration Compliance <i>Impact: High</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECSC-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Please see Appendix H, Q, and FF for ST&E and security test results.
M ECSD-1 Software Development Change Controls <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECSD-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Clean Test System	Compliant	Validated: SCRs procedures are addressed in the CM Plan. Please see SSAA Appendices.
M ECTM-1 Transmission Integrity Controls <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECTM-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Please refer to CCB documentation.
M ECTP-1 Audit Trail Protection <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECTP-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Audit trail permissions follow DoD policies, and are in accordance with the principle of "least privilege".
M ECVI-1 Voice-over-IP (VoIP) Protection <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECVI-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: VoIP traffic is expressly prohibited. Please refer to Appendix I, Section 12.
Validation Test : ECVI-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Not Applicable	Not applicable, as VoIP is prohibited.
M ECVP-1 Virus Computing <i>Impact: High</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECVP-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All system components have a waiver, evidence that virus protection is being acquired, or virus protection software installed and configured to utilize automatic updates as required by security policy. All virus protection software installed have signatures that are current as of the test date.
M ECWM-1 Warning Message <i>Impact: Basic</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : ECWM-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All system components have a waiver, evidence that virus protection is being acquired, or virus protection software installed and configured to utilize automatic updates as required by security policy. All virus protection software installed have signatures that are current as of the test date.

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

M	ECWN-1 Wireless Computing and Network <i>Impact: High</i>	Control Status: Compliant		POA&Ms Exist: No
Validation Test : ECWN-1-1				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: All system components with wireless computing and networking capabilities are implemented in accordance with DoD wireless policy, as issued. All wireless computing and networking capabilities are configured consistently.		
Validation Test : ECWN-1-2				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are disabled by changing factory defaults, settings or configurations prior to issue to end users.		

Subject Area: Identification and Authentication (IA)

M	IAKM-1 Key Management <i>Impact: Moderate</i>	Control Status: Compliant		POA&Ms Exist: No
Validation Test : IAKM-1-1				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: Symmetric keys are produced, controlled and distributed using NSA-approved key management technology; and asymmetric keys are produced, controlled and distributed using DoD PKI Class 3 or pre-placed keying material. Proper key management is in place.		
M	IATS-1 Token and Certificate Standards <i>Impact: Moderate</i>	Control Status: Compliant		POA&Ms Exist: No
Validation Test : IATS-1-1				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token.		

Subject Area: Personnel (PR)

M	PRMP-1 Maintenance Personnel <i>Impact: High</i>	Control Status: Compliant		POA&Ms Exist: No
Validation Test : PRMP-1-1				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: All maintenance personnel identified on the reviewed logs were authorized to conduct maintenance.		
Validation Test : PRMP-1-2				
Validation Test Status: Compliant				
System Name				
Clean Test System	Status	Comments		
	Compliant	Validated: A documented process for determining authorization to conduct maintenance exists.		
M	PRNK-1 Access to Need-to-Know Information <i>Impact: High</i>			

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Control Status: Compliant		POA&Ms Exist: No
Validation Test : PRNK-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: A tailored access roster based on need-to-know determination exists for each selected category.
M	PRRB-1 Security Rules of Behavior or Acceptable Use Policy <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PRRB-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. Security Rules of Behavior clearly delineates IA responsibilities and expected behavior and the consequences of inconsistent behavior or non-compliance. 2. Signed acknowledgement of the rules is a condition of access.
Subject Area: Physical and Environmental (PE)		
M	PEEL-1 Emergency Lighting <i>Impact: Basic</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PEEL-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.
M	PEFD-1 Fire Detection <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PEFD-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. Operational battery-operated or electric stand-alone smoke detectors are installed in the facility. 2. Smoke detectors are in working condition and have been checked at regular intervals prescribed by local policy. 3. Electric stand-alone smoke detectors have adequate emergency power in the case of the facility loosing power.
M	PEFI-1 Fire Detection <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PEFI-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. The facility has had periodic fire marshal inspections. 2. Identified deficiencies are promptly resolved.
M	PEFS-1 Fire Suppression <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PEFS-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments

Control Icon Key

Mandated: M

Upgraded: U

Added: A

Inherited: I

Self Assessment: SA

Scorecard Report

Generated on 08-May-2006 at 17:02.

Clean Test System	Compliant	Validated: 1. Handheld fire extinguishers or fixed fire hoses are available in key computing facilities should an alarm sound or a fire be detected and are fully functional. 2. A record exists documenting that the fire extinguishing equipment has been inspected on a regular basis in accordance with local policy.
M PEHC-1 Humidity Controls <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : PEHC-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: An operational humidity control system is installed in key computing facilities that provides alarms of fluctuations potentially harmful to personnel or equipment operation.
M PEMS-1 Master Power Switch <i>Impact: High</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : PEMS-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. A temperature control system is installed in computing facilities that provides an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected. 2. Adjustments to the heating and cooling systems may be made manually.
M PESL-1 Screen Lock <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : PESL-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. On the selected workstations a screen lock capability is enabled either by explicit user action or automatically self-activates after the workstation remains idle for a set period of time. 2. Screen locks are enabled and only authorized users via a unique authenticator regain access to the workstation. 3. Screen locks cover the entire visible area of the screen with an unclassified pattern, picture or graphic representation.
M PETC-1 Temperature Controls <i>Impact: Moderate</i>	Control Status: Compliant	POA&Ms Exist: No
Validation Test : PETC-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1. A temperature control system is installed in computing facilities that provides an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected. 2. Adjustments to the heating and cooling systems may be made manually.
M PETN-1 Environmental Control Training <i>Impact: Basic</i>		

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Control Status: Compliant		POA&Ms Exist: No
Validation Test : PETN-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Initial and periodic training in the operation of and response to the environmental controls of key computing facilities is conducted for assigned personnel.
M	PEVR-1 Voltage Regulators <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : PEVR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Automatic voltage control is implemented for the key IT assets within the inspected computing facilities.
Subject Area: Security Design and Configuration (DC)		
M	DCAR-1 Procedural Review <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCAR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Compliant
M	DCAS-1 Acquisition Standards <i>Impact: High</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCAS-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Not Applicable	This is a COTS product
Validation Test : DCAS-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	According to the SSAA, this system uses a Common Criteria approved OS.
M	DCBP-1 Best Security Practices <i>Impact: Moderate</i>	
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCBP-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Clean Test System	Compliant	Validated: The System Security Design document addresses all required best security practices based on the system's MAC and Confidentiality levels. For each best practice, the document either (1) Provides the rationale for not incorporating the identified practice or (2) Explains how the practice was incorporated into the system design. The system security documentation addresses potential identity management products that will be implemented to prevent unauthorized access to the system. Feature tests of the randomly selected sample of system components or nodes in which best security practices had been incorporated return positive results for implementation of the best practices.
M DCCB-1 Control Board <i>Impact: Moderate</i> Control Status: Non-Compliant POA&Ms Exist: No		
Validation Test : DCCB-1-1 Validation Test Status: Non-Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Non-Compliant	Validated: There is no specific Configuration Management plan as of yet.
Validation Test : DCCB-1-2 Validation Test Status: Non-Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Non-Compliant	Validated: There is no organized CCB for this system.
M DCCS-1 Configuration Specifications <i>Impact: High</i> Control Status: Compliant POA&Ms Exist: No		
Validation Test : DCCS-1-1 Validation Test Status: Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: All system IA and IA-enabled products for which DoD security governance is not available are configured and implemented securely in accordance with industry best practices (e.g., SANS, vendor security checklists).
M DCCT-1 Compliance Testing <i>Impact: Moderate</i> Control Status: Compliant POA&Ms Exist: No		
Validation Test : DCCT-1-1 Validation Test Status: Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: 1. The procedures for testing of patches, upgrades and new AIS applications prior to deployment are documented. 2. The procedures are being followed and testing results are documented in CCB documentation.
M DCDS-1 Dedicated IA Services <i>Impact: Moderate</i> Control Status: Compliant POA&Ms Exist: No		
Validation Test : DCDS-1-1 Validation Test Status: Compliant		
<u>System Name</u>	<u>Status</u>	<u>Comments</u>
Clean Test System	Compliant	Validated: Formal risk analysis reports were performed for all the IA services of the system and approved by the DoD Component CIO.

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

M	DCFA-1 Functional Architecture for AIS Applications <i>Impact: Moderate</i>		POA&Ms Exist: No
Control Status: Compliant			
Validation Test : DCFA-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	The system functional architecture describes all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface are identified	
Validation Test : DCFA-1-2			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	The system functional architecture describes all user roles required for access control and the access privileges assigned to each role	
Validation Test : DCFA-1-3			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	The system functional architecture describes all unique security requirements, including where they have been implemented within the system, their purpose, and technical details of their implementation (e.g., encryption key strength/algorithm for data at rest).	
Validation Test : DCFA-1-4			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	The system functional architecture describes all categories of sensitive information processed or stored by the system application, and their specific protection plans (e.g., Privacy Act, HIPAA).	
Validation Test : DCFA-1-5			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	The system functional architecture describes, in detail, the restoration priority of each subsystem, process, or information source.	
M	DCHW-1 HW Baseline <i>Impact: High</i>		POA&Ms Exist: No
Control Status: Compliant			
Validation Test : DCHW-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: All system hardware and software is documented. Changes to system baseline must be approved by the CCB prior to fielding on a production system.	
Validation Test : DCHW-1-2			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: Multiple copies of hardware baseline exist in various locations. At least one copy is kept in a fireproof container.	

Control Icon Key

Mandated: M

Upgraded: U

Added: A

Inherited: I

Self Assessment: SA

Scorecard Report

Generated on 08-May-2006 at 17:02.

M	DCID-1 Interconnection Documentation <i>Impact: High</i>	POA&Ms Exist: No	
Control Status: Compliant			
Validation Test : DCID-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System enclave is identified and well documented in the security documentation. There are no plans for future sites, however alternate sites have been identified and accounted for in the COOP.	
Validation Test : DCID-1-2			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System enclave is identified and well documented in the security documentation. There are no plans for future sites, however alternate sites have been identified and accounted for in the COOP.	
M	DCII-1 IA Impact Assessment <i>Impact: Moderate</i>	POA&Ms Exist: No	
Control Status: Compliant			
Validation Test : DCII-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System uses a Configuration Control Board in accordance with Configuration Management documentation	
M	DCIT-1 IA for IT Services <i>Impact: High</i>	POA&Ms Exist: No	
Control Status: Compliant			
Validation Test : DCIT-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System uses a Configuration Control Board in accordance with Configuration Management documentation	
M	DCMC-1 Mobile Code <i>Impact: Moderate</i>	POA&Ms Exist: No	
Control Status: Compliant			
Validation Test : DCMC-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System does not currently implement mobile code, nor will it in future iterations.	
Validation Test : DCMC-1-2			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: System does not, and will not, ever use mobile code.	
M	DCNR-1 Non-repudiation <i>Impact: Moderate</i>	POA&Ms Exist: No	
Control Status: Compliant			
Validation Test : DCNR-1-1			
Validation Test Status: Compliant			
System Name	Status	Comments	
Clean Test System	Compliant	Validated: As a DoD system, NIST approved FIPS 140-2 level security is used for all cryptographic exchange.	

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

M	DCPD-1 Public Domain Software Controls <i>Impact: Moderate</i> Control Status: Compliant	POA&Ms Exist: No
Validation Test : DCPD-1-1 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: In accordance with Section 5.2 of Appendix E to the SSAA, only Government approved and procured COTS will be used in the CTS system
M	DCPP-1 Ports, Protocols, and Services <i>Impact: Moderate</i> Control Status: Compliant	POA&Ms Exist: No
Validation Test : DCPD-1-1 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Only port traffic that is pertinent to the CTS will be acceptable. Other OS services, ports, and protocols have been disabled according to DISA hardening guidelines.
M	DCPR-1 CM Process <i>Impact: High</i> Control Status: Compliant	POA&Ms Exist: No
Validation Test : DCPR-1-1 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: A CM plan has been established that maintains control of any and all changes made to system software and hardware. This is in accordance with Section 6 of Appendix E to the SSAA.
M	DCSD-1 IA Documentation <i>Impact: High</i> Control Status: Compliant	POA&Ms Exist: No
Validation Test : DCSD-1-1 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: The CTS SSAA and its Appendices identify all IA personnel, all applicable Government policies, data handling and sensitivity, system redundancy and backup, as well as emergency response procedures. See the CTS SSAA main body, Appendix C, Appendix L.
Validation Test : DCSD-1-2 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Assigned IA personnel are documented, and are required to sign appointment letters. See Appendices AA and DD.
M	DCSL-1 System Library Management Controls <i>Impact: Moderate</i> Control Status: Compliant	POA&Ms Exist: No
Validation Test : DCSL-1 Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Any and all changes to the system, code, or system libraries must first pass through the CCB.
Validation Test : DCSL-1-1		

Control Icon Key

Mandated: **M**

Upgraded: **U**

Added: **A**

Inherited: **I**

Self Assessment: **SA**

Scorecard Report

Generated on 08-May-2006 at 17:02.

Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1) All system development is controlled by the CCB. 2) In accordance with Appendix E, Section 6, all system changes must pass through CCB first. 3) Again, all system changes are run through CCB, 4) Only appropriate developers are given access to the system source code.
M DCSQ-1 Software Quality <i>Impact: Moderate</i>		
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCSQ-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: All lifecycle documentation is recorded in the CTS SSAA.
Validation Test : DCSQ-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Yes, Recommended Standard Application Security Requirements are listed in Appendix H of the CTS SSAA
Validation Test : DCSQ-1-3		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Test plan includes DoD Internet Council Checklist.
M DCSR-1 Specified Robustness - Basic <i>Impact: High</i>		
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCSR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Given the Sensitive nature of the information handled by this system, all products exceed Basic Robustness requirements and are validated to EAL4+
M DCSS-1 System State Changes <i>Impact: High</i>		
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCSS-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: CTS is in compliance with DoD, DISA STIGS, and NSA guidelines in regards to system initialization, shutdown, and abort.
Validation Test : DCSS-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: Security scans are run on the enclave regularly, as is documented in the CTS SSAA.
M DCSW-1 SW Baseline <i>Impact: High</i>		
Control Status: Compliant		POA&Ms Exist: No
Validation Test : DCSW-1-1		

Control Icon Key

Mandated: M

Upgraded: U

Added: A

Inherited: I

Self Assessment: SA

Scorecard Report

Generated on 08-May-2006 at 17:02.

Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: A comprehensive list of all software including vendor, version number, license, and location is contained within the CTS SSAA.
Validation Test : DCSW-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: 1) All backups are stored offsite and in fireproof containers. 2) Backups are kept current. Certain software may require updates/upgrades/patches if reinstalled.

Subject Area: Vulnerability and Incident Management (VI)

M	VIIR-1 Incident Response Planning <i>Impact: High</i>	POA&Ms Exist: No
Control Status: Compliant		
Validation Test : VIIR-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Reviewed: 1. Incident Response Plan exists and defines incident categories. 2. Supporting TTPs exist and provide sufficient specific detail for foreseeable incidents. 3. Incident Response Team personnel are assigned in writing. 4. Assigned personnel are trained in incident response. 5. Users are training in incident recognition and initial notification.
Validation Test : VIIR-1-2		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Reviewed: The incident response plan is exercised at least annually.
Validation Test : VIIR-1-3		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Validated: The reviewed incidents were managed according to the procedures and requirements described in the Incident Response Plan.
M	VIVM-1 Vulnerability Management <i>Impact: Moderate</i>	POA&Ms Exist: No
Control Status: Compliant		
Validation Test : VIVM-1-1		
Validation Test Status: Compliant		
System Name	Status	Comments
Clean Test System	Compliant	Reviewed: The organization is in compliance with the DoD Information Assurance Vulnerability Management (IAVM) program and that a written and signed compliance policy is put into affect.

Control Icon Key

Mandated: M

Upgraded: U

Added: A

Inherited: I

Self Assessment: SA