



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE)

13 May 2021

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series with Software Release 6.6.0a

- References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 2," September 2017
(c) through (d), see Enclosure 1

1. Certification Authority. Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Department of Defense Information Network (DoDIN) products, Reference (b).

2. Conditions of Certification. The Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series with Software Release 6.6.0a, hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (b), as a Data Storage Controller (DSC) and is certified for joint use with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than the expiration date listed in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Table with 3 columns: Description, Operational Impact, Remarks. Rows include UCR Waivers (None), Conditions of Fielding (None), Open Test Discrepancies (COH-0771-001), and a specific discrepancy entry regarding RAID support.

(Table continues on next page.)

**Table 1. Conditions (continued)**

Description		Operational Impact	Remarks
<b>TDR#</b>	<b>Open Test Discrepancies (continued)</b>		
COH-0771-002	DAT-000120: Per the Vendor LoC, the SUT does not support CIFS/SMB1.	None with Change Requirement	On 2 March 2021, DISA adjudicated this discrepancy as a UCR Change Requirement
COH-0771-003	DAT-000550: DSCP tags are not configurable. The SUT supports DSCP marking on egress traffic, however the markings do not coincide with Section 6, Table 6.3-2 "Traffic Conditioning Specification". Observed traffic conformed to the Vendor-specified shaping plan. The shaping plan is not configurable through the administrative interface.	Minor with POA&M	On 2 March 2021, DISA adjudicated this discrepancy as Minor with Vendor POA&M.
COH-0771-004	DAT-000420: NIS not supported.	None with Change Requirement	On 2 March 2021, DISA adjudicated this discrepancy as a UCR Change Requirement
COH-0771-005	DAT-000430: NIS netgroups not supported.	None with Change Requirement	On 2 March 2021, DISA adjudicated this discrepancy as a UCR Change Requirement
COH-0771-006	DAT-000450: iSNS is not supported.	None with Change Requirement	On 2 March 2021, DISA adjudicated this discrepancy as a UCR Change Requirement
<b>LEGEND:</b>			
CIFS	Common Internet File System	NIS	Network Information Service
COH	Cohesity	POA&M	Plan of Action and Milestones
DAT	Data	RAID	Redundant Array of Independent Disks
DISA	Defense Information Systems Agency	SMB	Server Message Block
DSCP	Differentiated Services Code Point	SUT	System Under Test
iSNS	Internet Storage Name Service	TDR	Test Discrepancy Report
LoC	Letter of Compliance	UCR	Unified Capabilities Requirement

**3. Interoperability Status.** Table 2 provides the SUT interface interoperability status. Table 3 provides the Capability Requirements and Functional Requirements status, and Table 4 provides a DoDIN APL product summary, to include subsequent Desktop Review (DTR) updates.

**Table 2. SUT Interface Status**

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
<b>Network Attached Storage (NAS) Interfaces</b>			
1 GbE (Ethernet) (R)	1	Met	
10 GbE (Ethernet) (R)	1	Met	
<b>Storage Array Net (SAN) Interfaces</b>			
Fibre Channel (FC)(C)	1	Not Tested	The SUT does not support this conditional Interface.
FC Protocol (FCP)(C)	1	Not Tested	The SUT does not support this conditional Interface.

(Table continues on next page.)

JITC Memo, JTE, Joint Interoperability Certification of the Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series with Software Release 6.6.0a

**Table 2. SUT Interface Status (continued)**

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks
<b>Out-of-band Management Interfaces</b>			
10 Mbps Ethernet (R)	1	Not Tested	See note 2.
100 Mbps Ethernet (R)	1	Not Tested	See note 2.
1 GbE (O)	1	Met	
10 GbE (O)	1	Met	
<b>Converged Network Adapter (CNA) Interfaces</b>			
10 GbE (Ethernet) (O)	1	Not Tested	The SUT does not support this optional interface.
<b>NOTE(S):</b>			
1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.2.			
2. Testing was conducted on the higher data rate interfaces (1 and 10 GbE). JITC analysis determined the lower interface rates are low risk for certification based on the Vendor's LoC with the IEEE 802.3i and 802.3u standards and the testing data collected at all other data rates.			
<b>LEGEND:</b>			
802.3i	10BaseT 10 Mbps Ethernet over Twisted Pair	IEEE	Institute of Electrical and Electronics Engineers
80.23u	Fast Ethernet at 100 Mbps, copper and Fiber	JITC	Joint Interoperability Test Command
C	Conditional	LoC	Letters of Compliance
CNA	Converged Network Adapter	Mbps	Megabits per second
CR	Capability Requirement	NAS	Network Attached Storage
FC	Fiber Channel	O	Optional
FCP	Fiber Channel Protocol	R	Required
FR	Functional Requirement	SAN	Storage Array Network
GbE	Gigabit Ethernet	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements

**Table 3. SUT Capability Requirements and Functional Requirements Status**

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Data Storage Controller (DSC) (R)	Section 14	Partially Met (See note 2.)
2	IPv6	Section 5	Met
3	Cybersecurity	Section 4	Met (See note 3.)
<b>NOTE(S):</b>			
1. The annotation of 'required' refers to a high-level requirement category. Enclosure 3 provides the applicability of each sub-requirement.			
2. See Table 1 for SUT Conditions.			
3. USAISEC-TIC-led CS test team conducted CS testing and published the results in a separate report, Reference (c).			
<b>LEGEND:</b>			
CR	Capability Requirement	R	Required
CS	Cybersecurity	SUT	System Under Test
DSC	Data Storage Controller	TIC	Technology Integration Center
FR	Functional Requirement	UCR	Unified Capabilities Requirements
ID	Identification	USAISEC	U.S. Army Information Systems Engineering Command
IPv6	Internet Protocol version 6		

**Table 4. DoDIN APL Product Summary**

<b>Product Identification</b>			
Product Name	Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series		
Software Release	6.6.0a		
UCR Product Type(s)	Data Storage Controller		
Product Description	Cohesity Web-Scale Data Management Platform node provides compute, flash and HDD capacity to consolidate data and execute workflows. The Cohesity Web-Scale Data Management Platform with DataPlatform and DataProtect is used to hyperconverge secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may be distributed across multiple distributed appliances.		
<b>Product Components</b>	<b>Component Name</b> (See note 1.)	<b>Tested Version</b>	<b>Remarks</b>
Web-Scale Data Management Platform (See note 2.)	C4300 C4500 <b><u>C4600</u></b> C6025 C6035 C6045	<b><u>6.6.0a</u></b>	Hardware Node Block (See note 2.)
<b>NOTE(S):</b>			
1. Components bolded and underlined were tested by USAISEC-TIC. The specific node/model tested during initial certification was the C4600-SFP-4. The other components in the family series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested and certified components and JITC analysis determined they were functionally identical for interoperability certification purposes.			
2. The Web-Scale Data Management Platform is comprised of a Hardware Node Block with DataPlatform for provision of Distributed Storage Services and DataProtect for provision of Replication Services.			
<b>LEGEND:</b>			
APL	Approved Products List	SFP	Small Form-factor Pluggable
DoDIN	Department of Defense Information Network	TIC	Technology Integration Center
HDD	Hard Disk Drive	UCR	Unified Capabilities Requirements
JITC	Joint Interoperability Test Command	USAISEC	U.S. Army Information Systems Engineering Command

**4. Test Details.** This certification is based on interoperability testing, review of the Vendor’s Letters of Compliance (LoC), DISA adjudication of open test discrepancy reports (TDRs), and DISA Certifying Authority (CA) Recommendation for inclusion on the DoDIN APL. The United States Army Information Systems Engineering Command Technology Integration Center (USAISEC-TIC) completed review of the Vendor’s LoC on 5 February 2021 and conducted testing at the Technology Integration Center (TIC), Fort Huachuca, Arizona from 9 February 2021 through 12 February 2021, using test procedures derived from Reference (c). DISA adjudicated outstanding TDRs on 2 March 2021. A USAISEC-TIC-led Cybersecurity (CS) test team conducted CS testing and published the results in a separate report, Reference (d). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

**5. Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-but-Sensitive Internet Protocol Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at <https://stp.fhu.disa.mil/>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Industry Toolkit (JIT) at <https://jit.fhu.disa.mil/>. Due to the sensitivity of the information, the CS Assessment Package (CAP) that contains the approved configuration and deployment guide must be requested directly from the APCO via e-mail:

JITC Memo, JTE, Joint Interoperability Certification of the Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series with Software Release 6.6.0a

[disa.meade.ie.list.approved-products-certification-office@mail.mil](mailto:disa.meade.ie.list.approved-products-certification-office@mail.mil). All associated information is available on the DISA APCO website located at <https://aplits.disa.mil/>.

**6. Point of Contact (POC).** USAISEC-TIC Testing POC: Michelle W. Lavery; commercial telephone (520) 940-3250; email address: [michelle.w.lavery.civ@mail.mil](mailto:michelle.w.lavery.civ@mail.mil). JITC certification POC: Lisa Esquivel; commercial telephone (520) 538-5531; e-mail address: [lisa.r.esquivel.civ@mail.mil](mailto:lisa.r.esquivel.civ@mail.mil); mailing address: Joint Interoperability Test Command, ATTN: JTE (Lisa Esquivel), P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 2007701.

FOR THE COMMANDER:

3 Enclosures a/s

JEFFREY P. O'DONNELL  
LTC, USA  
Acting Chief  
Networks/Communications &  
DoDIN Capabilities Division

**Distribution (electronic mail):**

DoD CIO  
Joint Staff J-6, JCS  
ISG Secretariat, DISA, JT  
U.S. Strategic Command, J66  
USSOCOM J65  
USTRANSCOM J6  
US Navy, OPNAV N2/N6FP12  
US Army, DA-OSA, CIO/G-6, SAIS-CBC  
US Air Force, SAF/A6SA  
US Marine Corps, MARCORSSYSCOM, SEAL, CERT Division  
US Coast Guard, CG-64  
DISA/ISG REP  
OUSD Intel, IS&A/Enterprise Programs of Record  
DLA, Test Directorate, J621C  
NSA/DT  
NGA, Compliance and Assessment Team  
DOT&E  
Medical Health Systems, JMIS PEO T&IVV  
HQUSAISEC, AMSEL-IE-IS  
APCO

## **ADDITIONAL REFERENCES**

- (c) Joint Interoperability Test Command, “Data Storage Controller (DSC) Test Procedures Version 1.1 for Unified Capabilities Requirements (UCR) 2013 Change 2,” December 2020
- (d) U.S. Army Information Systems Engineering Command, Mission Engineering Directorate, Technology Integration Center (TIC) (USAISEC-MED-TIC), “Cybersecurity Assessment Report for Cohesity Web-Scale Data Management TN 2007701, Software Release 6.6.0a, Data Storage Controller (DSC), (Tracking Number 2007701), March 2021.

## CERTIFICATION SUMMARY

**1. SYSTEM AND REQUIREMENTS IDENTIFICATION.** The Cohesity Web-Scale Data Management Platform C4x00 Series and C60xx Series with Software Release 6.6.0a is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

**Table 2-1. System and Requirements Identification**

<b>System Identification</b>			
Sponsor	United States Army		
Sponsor Point of Contact	Jordan Silk, ELIE-ISE-TI, Address: 53302 Arizona Street, Fort Huachuca, Arizona 85613, E-mail: <a href="mailto:jordan.r.silk.civ@mail.mil">jordan.r.silk.civ@mail.mil</a>		
Vendor Point of Contact	Jeremy Duncan, Tachyon Dynamics, 335 South Centerville Parkway Suite D, Chesapeake, Virginia 23322, E-mail: <a href="mailto:jduncan@tachyondynamics.com">jduncan@tachyondynamics.com</a> Lintu Thomas, Sr., Director of Engineering, Cohesity, 300 Park Ave Suite 1700, San Jose, California, 95110, Email: <a href="mailto:lintu@cohesity.com">lintu@cohesity.com</a>		
System Name	Web-Scale Data Management Platform C4x00 Series and C60xx Series		
Increment and/or Version	6.6.0a		
Product Category	Data Storage Controller		
<b>System Background</b>			
Previous certifications	None		
<b>Tracking</b>			
APCO ID	2007701		
JITC STP ID	8508		
<b>Requirements Source</b>			
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 2, Sections 4,5,14		
Remarks	None		
<b>Test Organization(s)</b>	USAISEC-TIC		
<b>LEGEND:</b>			
APCO ID	Approved Products Certification Office\ Identification	SUT	System Under Test
JITC	Joint Interoperability Test Command	TIC	Technology Integration Center
STP	System Tracking Program	USAISEC	U.S. Army Information Systems Engineering Command

**2. SYSTEM DESCRIPTION.** A Data Storage Controller (DSC) is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (ASLAN); however, the DSC is not considered part of the ASLAN.

The SUT is a Data Storage Controller (DSC). Each Cohesity Web-Scale Data Management Platform node provides compute, flash and HDD capacity to consolidate data and execute workflows. The Cohesity Web-Scale Data Management Platform with DataPlatform and DataProtect is used to hyperconverge secondary storage workloads (i.e., enterprise data backups) into a single managed backup solution, which may be distributed across multiple distributed appliances. The intent of this product is to simplify the infrastructure and resources used to administer data backup and recovery functions across an enterprise. The product natively supports backups for various virtual machines, databases, and network-attached storage (NAS)

devices.

**3. OPERATIONAL ARCHITECTURE.** The Department of Defense Information Network (DoDIN) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DoDIN Capability (DC) architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational DoDIN architecture in which the SUT may be used and Figure 2-2 the DSC functional model.

**4. TEST CONFIGURATION.** The USAISEC-TIC tested the SUT at the TIC, Fort Huachuca, Arizona in a manner and configuration similar to that of the notional operational environment depicted in Figure 2-1. The test team verified the required functions and features of the SUT using the end-to-end test configuration depicted in Figure 2-3. The test team conducted interoperability testing of the SUT components by testing the SUT with different vendor DoDIN Approved Products List certified products. Cybersecurity (CS) testing used the same configuration.

**5. METHODOLOGY.** The USAISEC-TIC conducted testing using DSC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, reference (b), and DSC test procedures derived from reference (c). Test Discrepancy Reports (TDRs) document any noted discrepancies. The vendor submitted plan of action and milestones (POA&M) as required. The Defense Information Systems Agency (DISA) adjudicated the TDRs as minor. The Defense Information Systems Agency (DISA) will evaluate any new discrepancy noted in the operational environment for impact on the existing certification. DISA will adjudicate these discrepancies via a vendor POA&M, which must address all new critical TDRs within 120 days of identification.



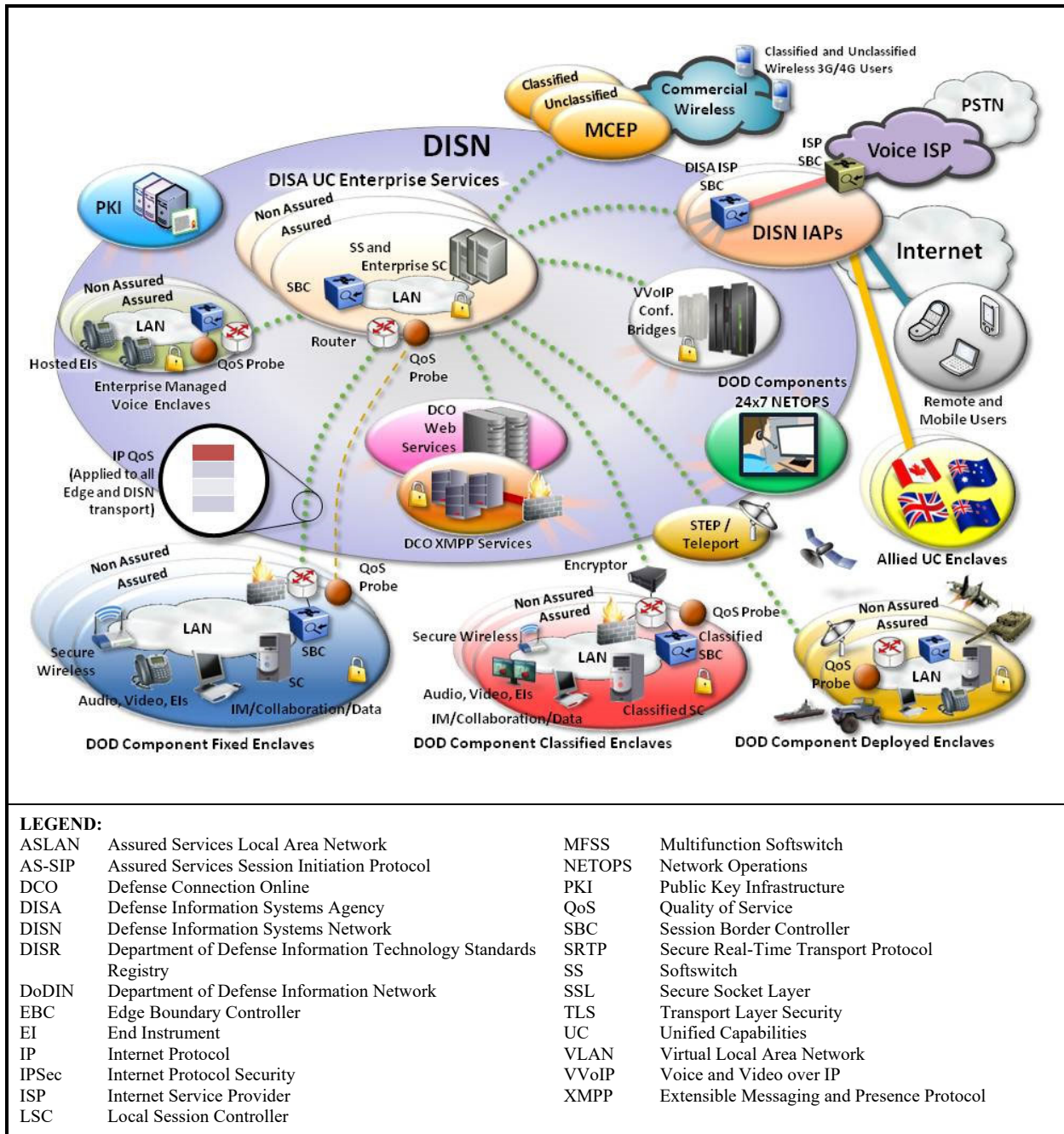
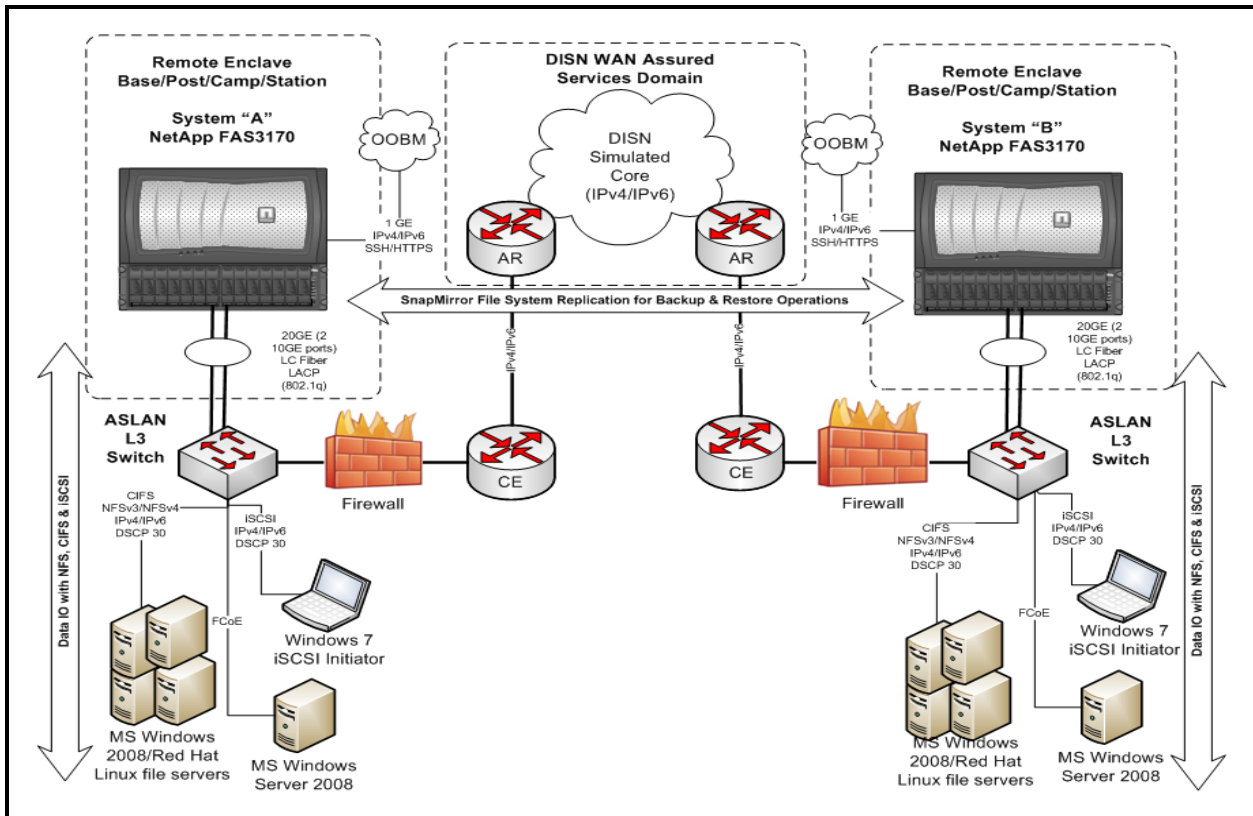


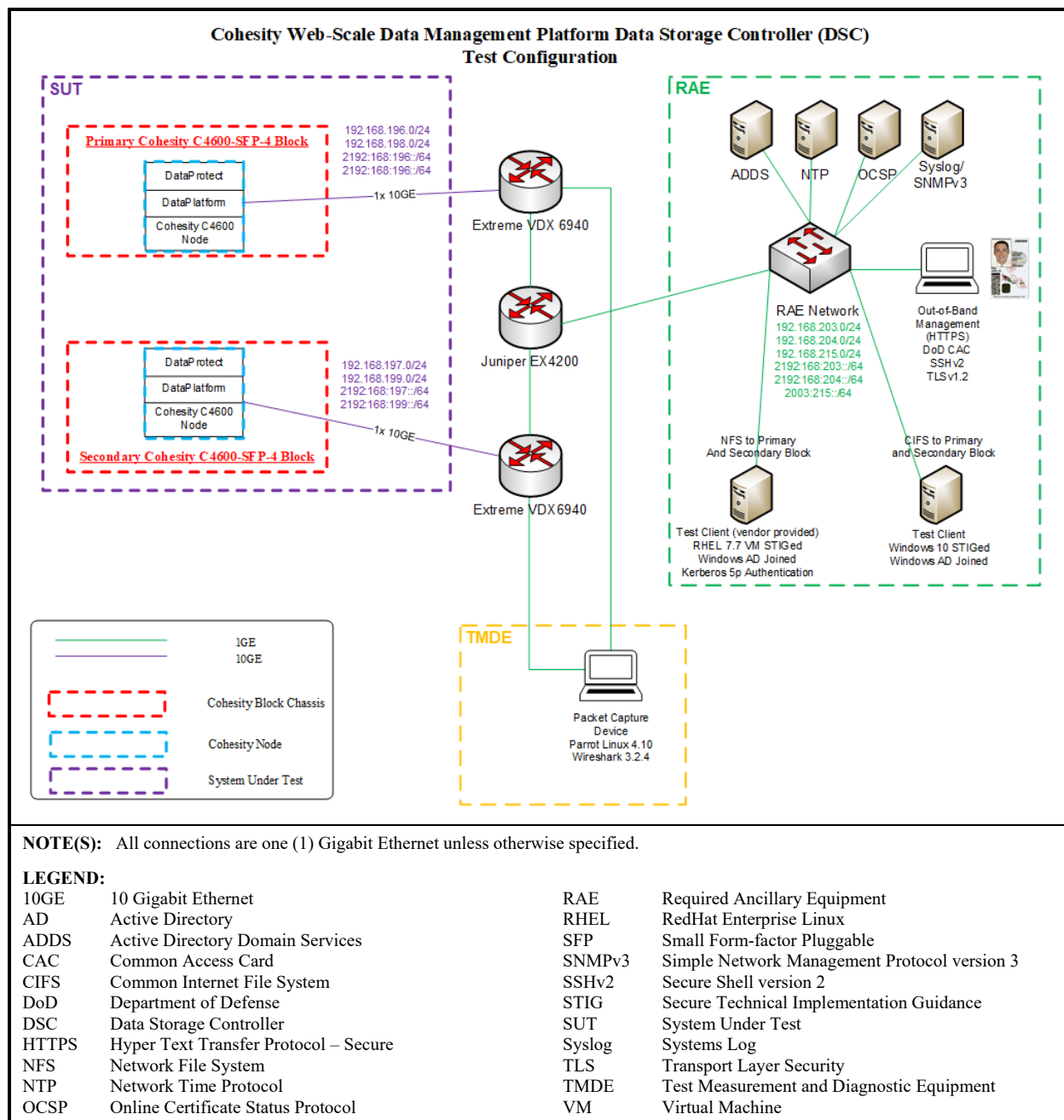
Figure 2-1. Notional DoDIN Network Architecture



**LEGEND:**

802.1q	VLAN Tagging	iSCSI	Internet Small Computer Systems Interface
AR	Aggregation Router	L3	Layer 3
ASLAN	Assured Services Local Area Network	LACP	Link Aggregation Control Protocol
CE	Customer Edge	LC	Lucent Connector
CIFS	Common Internet File System	MS	Microsoft
DISN	Defense Information Systems Network	NetApp	Network Application
DSCP	Differentiated Services Code Point	NFSv3	Network File System version 3
FCoE	Fibre Channel Over Ethernet	NFSv4	Network File System version 4
GE	Gigabit Ethernet	OoBM	Out of Band Management
HTTPS	Hypertext Transfer Protocol	SCSI	Small Computer System Interface
IO	Input Output	SSH	Secure Shell
IPv4	Internet Protocol version 4	VLAN	Virtual Local Area Network
IPv6	Internet Protocol version 6	WAN	Wide Area Network

**Figure 2-2. Data Storage Controller Functional Reference Model**



**Figure 2-3. SUT Test Configuration**

**6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS.** The interface, Capability Requirements (CR) and Functional Requirements (FR), and other requirements for DSCs are established by UCR 2013, Change 2, Section 14.2.

**a. Interface Status.** The USAISEC-TIC testing interface status of the SUT is provided in Table 3-1. The DSC shall provide physical interfaces for, at a minimum, 1 Gigabit Ethernet (GbE) and 10 GbE in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet Local Area Network (LAN) interfaces. The SUT met this interface requirement with testing. The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Megabit per second (Mbps) Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: Secure Shell version 2 (SSHv2), Transport Layer Security (TLS), Hyper Text Transfer Protocol Secure (HTTPS), and Simple Network Management Protocol (SNMP) version 3; and the protocols shall be secured in accordance with Section 4, Information Assurance. The SUT met this interface requirement with testing. The system may optionally provide Fiber Channel (FC) physical interfaces and FC Protocol (FCP) interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT does not support this optional interface requirement. The system may optionally provide physical interfaces for FC over Ethernet (FCoE) services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT does not support this optional interface requirement.

**b. Capability and Functional Requirements and Status.**

1) The UCR 2013, section 14.2 includes the Storage System requirements in the subparagraphs below.

a) The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and FC drives, although stronger RAID levels are acceptable. The SUT does not support RAID as a fault tolerance measure. The SUT implements Erasure Coding to prevent data loss in the event of disk failures. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1.

b) The system shall be capable of 99.9 percent availability. The SUT met this requirement with the Vendor's LoC.

c) The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner's (i.e., MILDEP) management network/LAN and also provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging. The SUT met this requirement with the Vendor's LoC.

d) The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning. The SUT met this requirement with testing and the Vendor's LoC.

e) When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC. The SUT met this requirement with testing and the Vendor's LoC.

f) The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information. The SUT met this requirement with testing and the Vendor's LoC.

g) The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP. The SUT met this requirement with testing and the Vendor's LoC.

h) The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in UCR 2013, Change 1, Table 14.2-1, Replication Operation Modes. The SUT met this requirement with testing and the Vendor's LoC.

2) The UCR 2013, section 14.3 includes the Storage Protocol requirements in the subparagraphs below.

a) The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O). The SUT met this requirement with testing and the Vendor's LoC.

b) The system shall provide a NFS version 4 (NFSv4) server for file systems data I/O. The SUT met this requirement with testing and the Vendor's LoC.

c) The system shall provide a NFS version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. The SUT met this requirement with testing and the Vendor's LoC.

d) The system shall provide a CIFS version 1.0 (CIFSv1.0) server for file systems data I/O. The SUT did not meet this requirement. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 of the certification memo.

e) The system shall provide a CIFS version 2.0 (CIFSv2.0) server for file systems data I/O. The SUT met this requirement with testing and the Vendor's LoC.

f) The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

g) The system shall provide FCP server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

h) The system shall provide FCoE server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

i) The system shall provide a HTTPS server for file system data I/O and management access to the storage controller operating system. The session shall be secured with SSL or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Information Assurance, for that protocol. The SUT met this requirement with the Vendor's LoC.

j) The system shall provide SSHv2 or TLS for management access to the storage controller operating system. The SSHv2 or TLS implementation shall comply with Section 4, Information Assurance, for that protocol. The SUT met this requirement with testing and the Vendor's LoC.

k) The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

l) The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

m) The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

n) The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS. The SUT met this requirement with testing and the Vendor's LoC.

3) The UCR 2013, section 14.4 includes the Network Attached Storage Interface requirements in the subparagraphs below.

a) The system shall provide physical interfaces for Gigabit Ethernet (GbE) and 10 Gigabit Ethernet (10 GbE) services in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces. The SUT met this requirement with testing for the 10 GbE interface and with the Vendor's LoC.

b) The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion. The SUT met this requirement with the Vendor's LoC.

c) The system shall provide physical interfaces for OOBM access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Cybersecurity. The SUT met this requirement with testing and the Vendor's LoC. A USAISEC-TIC-led CS test team conducted CS testing and published the results in a separate report, Reference (d).

d) When the system uses Ethernet, Fast Ethernet, GbE, and 10GbE interfaces, the interfaces shall be autosensing, auto-detecting, and auto-configuring with incoming and corresponding Ethernet link negotiation signals. Autosensing, auto-detecting, and auto-configuring only applies to interfaces below 10GbE interfaces. The SUT met this requirement with the Vendor's LoC.

e) Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3. The SUT met this requirement with the Vendor's LoC.

f) Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes. The SUT met this requirement with the Vendor's LoC.

g) Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q. The SUT met this requirement with the Vendor's LoC.

h) Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008, and use with the Link Aggregation Control Protocol. The SUT met this requirement with the Vendor's LoC.

i) Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

4) The UCR 2013, section 14.5, states the system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

5) The UCR 2013, section 14.6 includes the Converged Network Adapter Interface requirements in the subparagraphs below.

a) The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

b) The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

6) The UCR 2013, section 14.7 includes the IP Networking requirements in the subparagraphs below.

a) The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance. The SUT met this requirement with the Vendor's LoC.

b) The system shall provide statically provisioned or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically



provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session. The SUT met this requirement with the Vendor's LoC.

c) The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products. The SUT met this requirement with the Vendor's LoC.

7) The UCR 2013, section 14.8 includes the Name Services requirements in the subparagraphs below.

a) The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510. The SUT met this requirement with testing and the Vendor's LoC.

b) The system shall provide Kerberos authentication service per IETF RFC 4120. The SUT met this requirement with testing and the Vendor's LoC.

c) The system shall provide Domain Name System (DNS) client functionality. The SUT met this requirement with testing and the Vendor's LoC.

d) The system shall provide DNS client-side Load Balancing. The SUT met this requirement with testing and the Vendor's LoC.

e) The system shall provide Network Information Service (NIS) client directory service functionality. The SUT did not meet this requirement. DISA adjudicated this discrepancy as a UCR Change requirement, as noted in Table 1 of the certification memo.

f) The system shall provide NIS Netgroups client directory service functionality. The SUT did not meet this requirement. DISA adjudicated this discrepancy as a UCR Change requirement, as noted in Table 1 of the certification memo.

g) The system shall provide Network Basic Input/Output System (NETBIOS) over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

h) The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171. The SUT did not meet this requirement. DISA adjudicated this discrepancy as a UCR Change requirement, as noted in Table 1 of the certification memo.

i) If the system has a FC interface then the system shall provide FC Name and Zone Service. The SUT does not support this conditional requirement; therefore, it was not tested and is not included in this certification.

8) The UCR 2013, section 14.9 includes the Security Services requirements in the subparagraphs below.

a) The system shall provide IPSec per RFC 4301. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

b) The system shall provide Encapsulating Security Payload (ESP) per RFC 4303. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

c) The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

d) The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a “stateless” design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

e) The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities:

1. Rapid crypto-shredding (destruction) of data, in accordance with National Institute of Standards and Technology 800-88, for tactical systems that operate in harm’s way and may fall into enemy hands. The SUT met this requirement with the Vendor’s LoC.

2. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place. The SUT met this requirement with the Vendor’s LoC.

f) The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide. A USAISEC-TIC-led CS test team conducted CS testing and published the results in a separate report, Reference (c).

9) The UCR 2013, section 14.10, states the system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation. The SUT met this requirement with the Vendor’s LoC.

10) The UCR 2013, section 14.11 includes the Class of Service and Quality of Service requirements in the subparagraphs below.

a) The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

b) The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1. The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements. The SUT partially met this requirement. DISA adjudicated this discrepancy as Minor with Vendor POA&M, as noted in Table 1 of the certification memo.

11) The UCR 2013, section 14.12 includes the Virtualization requirements in the subparagraphs below.

a) The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

b) The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

c) The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

d) The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context. The SUT

does not support this optional requirement; therefore, it was not tested and is not included in this certification.

e) The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration, and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical network access server heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system. The SUT does not support this optional requirement; therefore, it was not tested and is not included in this certification.

**7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION.** Table 3-3 provides the SUT components' hardware, software, and firmware tested. USAISEC-TIC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

**8. TESTING LIMITATIONS.** None

**9. CONCLUSION(S).** The SUT meets the critical interoperability requirements for a Data Storage Controller in accordance with the UCR and is certified for joint use with other DoDIN Products listed on the Approved Products List (APL). The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

## DATA TABLES

**Table 3-1. SUT Interface Status**

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks																																								
<b>Network Attached Storage (NAS) Interfaces</b>																																											
1 GbE (Ethernet) (R)	1	Met																																									
10 GbE (Ethernet) (R)	1	Met																																									
<b>Storage Array Net (SAN) Interfaces</b>																																											
Fibre Channel (FC)(C)	1	Not Tested	The SUT does not support this conditional interface.																																								
FC Protocol (FCP)(C)	1	Not Tested	The SUT does not support this conditional interface.																																								
<b>Out-of-band Management Interfaces</b>																																											
10 Mbps Ethernet (R)	1	Not Tested	See note 2.																																								
100 Mbps Ethernet (R)	1	Not Tested	See note 2.																																								
1 GbE (O)	1	Met																																									
10 GbE (O)	1	Met																																									
<b>Converged Network Adapter (CNA) Interfaces</b>																																											
10 GbE (Ethernet) (O)	1	Not Tested	The SUT does not support this optional interface.																																								
<p><b>NOTE(S):</b></p> <p>1. The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.</p> <p>2. Testing was conducted on the higher data rate interfaces (1 and 10 GbE), JITC analysis determined the lower interface rate are low risk for certification without testing based on the Vendor's Letters of Compliance (LoC) compliance with the IEEE 802.3i and 802.3u standards and the testing data collected at all other data rates.</p>																																											
<p><b>LEGEND:</b></p> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">802.3i</td> <td style="width: 33%;">10BaseT 10 Mbps Ethernet over Twisted Pair</td> <td style="width: 33%;">IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> </tr> <tr> <td>802.3u</td> <td>Fast Ethernet at 100 Mbps, copper and Fiber</td> <td>JITC</td> <td>Joint Interoperability Test Command</td> </tr> <tr> <td>C</td> <td>Conditional</td> <td>LoC</td> <td>Letters of Compliance</td> </tr> <tr> <td>CNA</td> <td>Converged Network Adapter</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>NAS</td> <td>Network Attached Storage</td> </tr> <tr> <td>FC</td> <td>Fibre Channel</td> <td>O</td> <td>Optional</td> </tr> <tr> <td>FCP</td> <td>Fibre Channel Protocol</td> <td>R</td> <td>Required</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SAN</td> <td>Storage Array Network</td> </tr> <tr> <td>GbE</td> <td>Gigabit Ethernet</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>				802.3i	10BaseT 10 Mbps Ethernet over Twisted Pair	IEEE	Institute of Electrical and Electronics Engineers	802.3u	Fast Ethernet at 100 Mbps, copper and Fiber	JITC	Joint Interoperability Test Command	C	Conditional	LoC	Letters of Compliance	CNA	Converged Network Adapter	Mbps	Megabits per second	CR	Capability Requirement	NAS	Network Attached Storage	FC	Fibre Channel	O	Optional	FCP	Fibre Channel Protocol	R	Required	FR	Functional Requirement	SAN	Storage Array Network	GbE	Gigabit Ethernet	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements
802.3i	10BaseT 10 Mbps Ethernet over Twisted Pair	IEEE	Institute of Electrical and Electronics Engineers																																								
802.3u	Fast Ethernet at 100 Mbps, copper and Fiber	JITC	Joint Interoperability Test Command																																								
C	Conditional	LoC	Letters of Compliance																																								
CNA	Converged Network Adapter	Mbps	Megabits per second																																								
CR	Capability Requirement	NAS	Network Attached Storage																																								
FC	Fibre Channel	O	Optional																																								
FCP	Fibre Channel Protocol	R	Required																																								
FR	Functional Requirement	SAN	Storage Array Network																																								
GbE	Gigabit Ethernet	SUT	System Under Test																																								
ID	Identification	UCR	Unified Capabilities Requirements																																								

**Table 3-2. Capability and Functional Requirements and Status**

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status																												
1	<b>Data Storage Controller (DSC) (R)</b>																														
	Storage System (R)	14.2	Met																												
	Storage Protocol (R)	14.3	Partially Met (See note 2.)																												
	Network Attached Storage Interface (R)	14.4	Met																												
	Storage Array Network Interface (O)	14.5	Not Tested (See note 3.)																												
	Converged Network Adapter Interface (O)	14.6	Not Tested (See note 3.)																												
	IP Networking (R)	14.7	Met																												
	Name Services (R)	14.8	Partially Met (See note 4.)																												
	Security Services (R)	14.9	Met (See note 5.)																												
	Interoperability (R)	14.10	Met																												
	Class of Service and Quality of Service (R)	14.11	Partially Met (See note 6.)																												
Virtualization (O)	14.12	Not Tested																													
<p><b>NOTE(S):</b></p> <ol style="list-style-type: none"> <li>1. The annotation of 'required' refers to a high-level requirement category.</li> <li>2. The SUT did not meet CIFS/SMB requirement. DISA adjudicated this discrepancy as a UCR Change Requirement, as noted in Table 1 of the certification memo.</li> <li>3. The SUT does not support this optional requirement.</li> <li>4. The SUT did not meet NIS and NIS netgroups requirements. DISA adjudicated this discrepancy as a UCR Change requirement, as noted in Table 1 of the certification memo.</li> <li>5. A USAISEC-TIC-led CS test team conducted CS testing and published the results in a separate report, Reference (c)</li> <li>6. The SUT partially met CoS and QoS requirements. DISA adjudicated this discrepancy as Minor with Vendor POA&amp;M, as noted in Table 1 of the certification memo.</li> </ol> <p><b>LEGEND:</b></p> <table border="0"> <tr> <td>CIFS</td> <td>Common Internet File System</td> <td>NIS</td> <td>Network Information Service</td> </tr> <tr> <td>CR</td> <td>Capability Requirement</td> <td>O</td> <td>Optional</td> </tr> <tr> <td>CS</td> <td>Cybersecurity</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DSC</td> <td>Data Storage Controller</td> <td>SMB</td> <td>Server Message Block</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>TIC</td> <td>Technology Integration Center</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>				CIFS	Common Internet File System	NIS	Network Information Service	CR	Capability Requirement	O	Optional	CS	Cybersecurity	R	Required	DSC	Data Storage Controller	SMB	Server Message Block	FR	Functional Requirement	SUT	System under Test	ID	Identification	TIC	Technology Integration Center	IP	Internet Protocol	UCR	Unified Capabilities Requirements
CIFS	Common Internet File System	NIS	Network Information Service																												
CR	Capability Requirement	O	Optional																												
CS	Cybersecurity	R	Required																												
DSC	Data Storage Controller	SMB	Server Message Block																												
FR	Functional Requirement	SUT	System under Test																												
ID	Identification	TIC	Technology Integration Center																												
IP	Internet Protocol	UCR	Unified Capabilities Requirements																												

**Table 3-3. SUT Hardware/Software/Firmware Version Identification**

<b>Components</b> (See note 1.)	<b>Release</b>	<b>Sub-component</b>	<b>Function</b>												
C4300 C4500 <b><u>C4600</u></b> C6025 C6035 C6045	<b><u>6.6.0a</u></b>	N/A	Hardware Node Block (See note 2.)												
<p><b>NOTE(S):</b></p> <p>1. Components bolded and underlined were tested by USAISEC-TIC. The specific node/model tested during initial certification was the C4600-SFP-4. The other components in the family series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested and certified components and JITC analysis determined they were functionally identical for interoperability certification purposes.</p> <p>2. The Web-Scale Data Management Platform is comprised of a Hardware Node Block with DataPlatform for provision of Distributed Storage Services and DataProtect for provision of Replication Services.</p> <p><b>LEGEND:</b></p> <table border="0"> <tr> <td>JITC</td> <td>Joint Interoperability Test Command</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>N/A</td> <td>Not Applicable</td> <td>TIC</td> <td>Technology Integration Center</td> </tr> <tr> <td>SFP</td> <td>Small Form-factor Pluggable</td> <td>USAISEC</td> <td>U.S. Army Information Systems Engineering Command</td> </tr> </table>				JITC	Joint Interoperability Test Command	SUT	System Under Test	N/A	Not Applicable	TIC	Technology Integration Center	SFP	Small Form-factor Pluggable	USAISEC	U.S. Army Information Systems Engineering Command
JITC	Joint Interoperability Test Command	SUT	System Under Test												
N/A	Not Applicable	TIC	Technology Integration Center												
SFP	Small Form-factor Pluggable	USAISEC	U.S. Army Information Systems Engineering Command												

**Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification**

System Name	Software Release	Function	
<b>Required Ancillary Equipment</b>			
Active Directory			
Network Time Protocol Server			
Public Key Infrastructure/Online Certificate Status Protocol Services			
Simple Network Management Protocol Version 3 Services			
Syslog Server			
<b>Test Network Components</b>			
Out-of-Band Management Workstation	Microsoft Windows 10	Management	
Test, Measurement, and Diagnostic Equipment	Parrot Linux version 4.10	TMDE	
Test Client (Site provided)	Red Hat Enterprise Linux version 7.7	NFS Test Client	
Test Client	Windows 10	CIFS Test Client	
Extreme VDX 6940	7.0.0a	Switching and Routing Services	
Juniper EX4200	12.3R12.4	Switching and Routing Services	
<b>LEGEND:</b>			
CIFS	Common Internet File System	Syslog	System Log
NFS	Network File System	TMDE	Test, Measurement, and Diagnostic Equipment
R	Release		