

Defense Critical Infrastructure Program Integrated Enterprise Architecture

Technology Standards Profile (TV-1)



June 30, 2006

DCIP Technology Standards Profile (TV-1)

Revision Sheet

Version No.	Date	Revision Description
1.0	6/30/2006	Final release

DCIP Technology Standards Profile (TV-1)

Table of Contents

1 Introduction.....	1
2 Shared Data Environment Characteristics and Requirements.....	1
3 DCIP Technology Standards	2
Section I - Standards	2
Section II: Policies & Guidance.....	7

DCIP Technology Standards Profile (TV-1)

1 INTRODUCTION

The Department of Defense Architectural Framework (DoDAF) Technical Views (TV) contain the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. The purpose of these rules is to ensure that a system satisfies a specified set of operational requirements. Technical Views provide detailed systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. Each Technical View includes a collection of technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture.

The Technical Standards Profile (TV-1) collects the various systems standards rules that implement and may sometimes constrain the choices that can be made in the design and implementation of architecture. Primarily, this view is concerned with delineating systems standards rules and conventions that apply to architecture implementations.

The TV-1 for the Defense Critical Infrastructure Program (DCIP) Shared Data Environment (SDE) will serve as the technical end-state for the Target Integrated Enterprise Architecture. It will consist of the set of systems standards rules that will govern funding of DCIP system implementation and operations of modernization architecture. The technical standards generally govern what hardware and software may be implemented and what system data formats may be used (i.e., the profile delineates which standards may be used to implement the systems, system hardware/software items, communications protocols, and system data formats). This DCIP SDE TV-1 also references the DCIP Metadata Definitions that will be developed and registered in accordance with the DoD Discovery Metadata Specifications (DDMS).

2 SHARED DATA ENVIRONMENT CHARACTERISTICS AND REQUIREMENTS

In order to select the appropriate standards that will be applied to the SDE, a number of characteristics and requirements had to be defined. The following table contains those assumptions about the overall structure and operation of the SDE.

SDE Characteristics

- HTML used will evolve into XML applications
- Share terrorism information with the justice and public safety communities
- Internet-based environment can be classified as a "stressed" communications environment
- Include a Relational DBMS (RDBMS) or use RDBMS resources
- Provide a Microsoft Windows (or Windows compliant) user interface
- Share terrorist person data
- Share information on terrorism operations or terrorists
- Transfer stored ISR data
- Automatically process or disseminate terrorism information across security domains

SDE Requirements

- Read/write random access to XML documents
- Industry-developed open standards will be used to ensure interoperability and to comply with DoD directives specifying the use of COTS and open industry developed standards
- Will comply with DoD Data Definitions

DCIP Technology Standards Profile (TV-1)

Data will be extracted from collections of XML documents using a flexible query facility
 XML DTD's will be used to exchange UML information
 Subnets will require LAN technology for joint interoperability using IPv6
 TCP transport policy will be managed via SNMP
 UDP transport QOS and policy will be managed via SNMP
 Connect to the Internet
 Contain host system implementations of the Internet Protocol (IP) suite
 A Domain Name Service for host name/IP address resolution for IPv4 & IPv6 will be required
 An ftp facility for IPv4 & IPv6 will be required
 Directory services for the location of users and resources on the network will be required
 Lightweight Directory Access Protocol Version 3 will be required
 Medium-assurance messaging services using SMTP will be required
 The syntax of URLs and URIs for IPv4 and IPv6 will be used
 Exchange documents in HTML format (including web publication)
 Exchange documents in XML format
 Calendaring and scheduling services
 Data interoperability
 Date format standards to be captured in FIPS 4-2 format
 Exchanging information in a decentralized distributed format
 Guaranteed delivery services from the GIG BE, preemption services from the GIG-BE, or sets the DiffServ Code Points or TOS bits in the IP Datagram
 Services that model some of their communication patterns as pure data-centric exchange
 Services to support the creation and manipulation of graphics
 File format, known as LDIF, for LDAP Data Interchange Format
 Use of the Internet Protocol (IP) for IPv6
 Use of the Transmission Control Protocol (tcp)
 Support the Simple Network Management Protocol (SNMP) version 2
 XML documents require an XML-encoded digital signature rather than as separate data
 Geospatial data in geographic databases intended for direct use
 Raster-formatted geospatial data
 Transform XML through the use of Style Sheets
 SNMP management for IPv6 based IT infrastructure
 Process WWW metadata
 Implement SQL remote database access (RDA)
 Provide an integrated environment for education, training, and decision support

3 DCIP TECHNOLOGY STANDARDS

Section I - Standards		
Category	Service	Standards
Business Processing	Calendaring and Scheduling	ANSI X3.30:1997
		C321
Environment Management	Learning Technologies	IEEE 1484.1 d9
		IEEE 1484.11.1
		IEEE 1484.12.1
	Transaction Processing	IETF RFC 2439

DCIP Technology Standards Profile (TV-1)

Category	Service	Standards
		IETF RFC 2918
Engineering Support		
	Modeling and Simulation	ISO/IEC 11179
		XMI, XMI-ax
User Interface Services		
		Win32 APIs-Current
Data Management Services		
	Database Management System	ANSI X3.135.10
		ISO/IEC 9075
		ISO/IEC 9075-1
		ISO/IEC 9075-2
		ISO/IEC 9075-3:1999
		ISO/IEC 9075-4
		ISO/IEC 9075-5
		ISO/IEC 9579:2000
		ISO 23950/NISO Z39.50
Data Interchange Services		
	Electronic Data Interchange (EDI)	XML Signature
	Document Interchange	HTML 4.01
		XHTML 1.1:31 May 2001
		XForms 1.0
		WSDL 1.1
		XML 1.1:2004
		RDF Vocabulary Description Language 1.0: RDF Schema
		RDF/XML Syntax Specification (Revised)
		SOAP 1.1
		SOAP 1.2
		XSL 1.0:2001
		XPath 1.0
		XPath 2.0
		DOM 1.0
		XQuery 1.0
		MIMOSA OSA-EAI:2004
		IISS GJXDM
		IISS ISM
		IISS RM:MES
		IISS Tearlines
		IISS Tearlines:XML
		IISS WPDE
	Mapping (Geospatial)	MIL-STD-2411(2)

DCIP Technology Standards Profile (TV-1)

Category	Service	Standards
		MIL-STD-2407(1)
	Application-specific Data Interchange	STANAG 4575
		OMG ptc/03-07-07
		DDMS
Graphics Services		
		ANSI/ISO/IEC 9636
		OpenGL Graphics:2001
Platform Communication Services		
	Platform Communications Services	IETF RFC 1995
		IETF RFC 1996
		IETF RFC 2136
		IETF Standard 13/RFC 1034/RFC 1035
		ITU-T X.500:2001
		IETF RFC 3377
		IETF RFC 2589
		IETF RFC 2849
	Network Technologies	IETF Standard 3/ RFC 1122/RFC 1123
		IETF RFC 1870
		IETF RFC 2231
		IETF RFC 2821
		IETF RFC 2822
		IETF RFC 3023
		IETF RFCs 2045-49
		ITU-T X.500:2001
		IETF RFC 1995
		IETF RFC 1996
		IETF RFC 2136, IETF Standard 13/RFC 1034/rfc 1035
		IETF Standard 13/RFC 1034/rfc 1035
		IETF Standard 9/RFC 959
		IETF RFC 2428
		IETF RFC 3384
		IETF RFC 3673
		IETF RFC 2616
		IETF RFC 1738
		IETF Standard 66/RFC 3986
		IETF RFC 2581
		IETF Standard 7/RFC 793

DCIP Technology Standards Profile (TV-1)

Category	Service	Standards
		IETF RFC 2794
		IETF RFC 3344
		IETF Standard 5
		IETF RFC 1981
		IETF RFC 2460
		IETF RFC 2461
		IETF RFC 2462
		IETF RFC 2463
		IETF RFC 2473
		IETF RFC 3513
		IETF RFC 2507
		IETF RFC 2466
		IETF RFC 2492
		IETF RFC 3041
		IETF RFC 3162
		IETF RFC 2508
		IETF RFC 3173
		IETF RFC 3544
		IETF RFC 3595
		IETF RFC 3596
		IETF RFC 3697
		IETF RFC 4213
		IETF RFC 4007
		CCSDS 713.0-B-1/ISO 15891:2000
		CCSDS 714.0-B-1/ISO 15893:2000
		CCSDS 717.0-B-1/ISO 15894:2000
		CCSDS 713.5-B-1/ISO 15892:2000
		IETF RFC 2464
		IETF Standard 62/IETF RFC 3416
		IETF RFC 4022
		IETF RFC 4113
		IETF RFC 2465
Security Services		
	Access Control	FIPS PUB 140-2, FIPS PUB
		IETF RFC 2630
		IETF RFC 2632
		IETF RFC 2634
		FIPS PUB 186-2
		FIPS Pub 180-2
	Architectures and Applications	OMG UML 1.5
		OMG UML 2.0
		OMG document formal/02-03-11

DCIP Technology Standards Profile (TV-1)

Category	Service	Standards
	Information System Security Management	IETF RFC 3414
		IETF RFC 3585
		IETF RFC 3566
		IETF RFC 3602, IETF RFC 3686
		IETF RFC 3664, IETF RFC 3526
	Security Protocols	IETF RFC 2246
		SSL
		IETF RFC 2228
		CIMCPP
		IETF RFC 2403
	System Management Services	IETF RFC 3411
		IETF RFC 3412
		IETF RFC 3413
		IETF Standard 15/RFC 1157
		IETF Standard 16/RFC 1155/RFC
		IETF RFC 1850, IETF Standard 17/RFC 1213, IETF Standard 59/RFC 2819, IETF RFC 2790
		IETF Standard 17/RFC 1213
		IETF Standard 59/RFC 2819
		IETF RFC 2790
		IETF RFC 3376
Operating System Services		
		C808, IEEE 1003.1j:2000
		IEEE 1003.2d
		IEEE 1003.1d
		ISO/IEC 9945-1
		ISO/IEC 9945- 1:2003 (Base Definitions)
		ISO/IEC 9945- 1:Thread
		ISO/IEC 9945- 2:2003
		ISO/IEC 9945- 3:2003
		P1003.21 v3
		ISO/IEC 14519
		Win32 APIs-Current
		UNIX Version 3

DCIP Technology Standards Profile (TV-1)

Category	Service	Standards
Web Services		
		IETF RFC 1738
		IETF RFC 2616
		CSS2:1998, XHTML 1.1, XSLT 2.0:2005
		XHTML 1.1
		XSLT 2.0:2005
		DOM Level 3 W3C
		XML 1.1:2004
		XML 1.0 (Third Edition)
		XSLT 2.0:2003
		XPATH 2.0
		IETF RFC 2560
		RBAC
		XACML 1.0 OASIS
		SPML v1.0
		UDDI 3.0.2
		IETF RFC 2965
		JSR 168
		OMG UML 1.5, OMG UML 2.0
		OWL
		WS-I Basic Profile 1.0
		WS-I Basic Profile 1.1
		WS-Security 1.0 OASIS
		ISO 15836:2003

Section II: Policies & Guidance		
DoD Policies	Policy/Guidance	Description
	Homeland Security Presidential Directive (HSPD) Number 7, "Critical Identification, Prioritization, and Protection," December 17, 2003.	Establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.
	Executive Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council," October 8, 2001	Establishes the Office of Homeland Security (predecessor organization to DHS within the Executive Office of the President, and defines its missions, functions, and administration.
	Directive 5220.22, "DoD Industrial Security Program," December 8, 1980	Assigns overall responsibility for policy and administration of the National Industrial Security Program (NISP) to ensure that classified

DCIP Technology Standards Profile (TV-1)

Section II: Policies & Guidance		
DoD Policies	Policy/Guidance	Description
		information released to industry is properly safeguarded.
	DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005	Updates policy, and assigns responsibilities for the Defense Critical Infrastructure Program (DCIP], incorporating guidance from the President in reference (b) to function as <i>the</i> Sector-Specific Agency for the Defense Industrial Base (DIB)
ASD (HD) DCIP Guidance	Policy/Guidance	Description
	DCIP Shared Data Environment Metadata Definitions	This document contains the DDMS metadata definitions that are registered with the Metadata Registry